Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2006/300146

International filing date: 10 January 2006 (10.01.2006)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2005-003596
Filing date: 11 January 2005 (11.01.2005)

Date of receipt at the International Bureau: 07 April 2006 (07.04.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００５年　１月１１日
出 願 番 号 Application Number:	特願２００５－００３５９６
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００５－００３５９６
出 願 人 Applicant(s):	松下電器産業株式会社

２００６年　３月２３日

特許庁長官
Commissioner,
Japan Patent Office

中嶋 誠

【書類名】　特許願
【整理番号】　7048060184
【提出日】　平成17年 1月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 11/14
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　田靡　雅基
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　佐藤　光弘
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　竹内　康雄
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　鶴切　恵美
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
外部機器からの指示を受けてカード発行を行うセキュアデバイスであって、
前記セキュアデバイスは、
前記カード発行のためのコマンド群を保持するコマンド格納部と、
前記セキュアデバイスの動作を管理するカード管理部と、
前記外部機器からの指示を受けて、前記コマンド格納部が保持するコマンド群にもとづいて、前記指示を満たす一連の発行コマンドを選択、構築するカード発行部と、
を備え、
カード発行は、
前記カード発行部による前記発行コマンドの出力と、
前記発行コマンドを受けたカード管理部によるレスポンスと、
からなる、セキュアデバイス内部の通信のみによって実行され、
前記カード管理部は、発行処理結果を前記外部機器に対し出力することを特徴とするセキュアデバイス。
【請求項２】
前記外部機器からの指示がカード発行要求かそれ以外かを判別し、カード発行要求の場合は、カード発行実行中は前記外部機器に発行処理結果を出力することができない特権モードを前記カード管理部に設定する特権モード管理部を更に備えることを特徴とする請求項１に記載のセキュアデバイス。
【請求項３】
前記特権モード管理部は、前記カード発行が成功したことを確認した場合または、前記カード発行が途中で失敗した場合に、前記特権モードを解除することを特徴とする請求項２に記載のセキュアデバイス。
【請求項４】
前記カード発行部は、カード発行の進捗状態を逐次、記憶し、カード発行の失敗を検出した場合は、失敗を意味する旨と発行処理の進捗状態とを、前記外部機器に出力することを特徴とする請求項１に記載のセキュアデバイス。
【請求項５】
通信接続されたセキュアデバイスに対しカード発行を指示する外部端末であって、
発行処理の進捗状態を、前記セキュアデバイスから受け取るレスポンス受信部と、
前記発行処理の進捗状態に対応する該外部機器の動作を決定するセルフ発行管理部と、
前記セルフ発行管理部からの指示を受けて前記セキュアデバイスに対するコマンドを生成するコマンド生成部と、
前記コマンド生成部により生成されたコマンドを前記セキュアデバイスに送信するコマンド送信部と、
を備えたことを特徴とする外部機器。
【請求項６】
前記コマンド格納部の発行コマンドを格納する領域を、直接アクセス可能な直接参照手段を更に設け、
前記指示がカード発行を意味する場合に、前記カード管理部が、前記直接参照手段を介して前記領域から発行コマンドを取得することを特徴とする請求項１に記載のセキュアデバイス。
【請求項７】
前記カード管理部は、カード発行が中断したときの進捗状況を前記カード発行部に送る中断履歴送信手段を有し、
前記カード管理部は、前記中断履歴送信手段から受信した進捗状況をもとに最初に処理するべき発行コマンドを選択、構築するリカバリ手段を有することを特徴とする請求項１に記載のセキュアデバイス。

【書類名】明細書
【発明の名称】セキュアデバイス及び外部機器
【技術分野】
【０００１】
本発明は、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）カードに代表されるセキュアデバイス並びに、セキュアデバイスに接続される携帯端末に代表される外部機器に関するものである。特に、通信接続された外部機器からの指示を受けて自立的にカード発行処理を行うセキュアデバイスに関するものである。
【背景技術】
【０００２】
現在セキュリティデバイスとしてＩＣカードが着目されている。ユーザの利便性の向上、ＩＣカードによるサービスを提供したい事業者の参入障壁を下げることを目的に、カード発行後にアプリケーションをダウンロードすることが可能なマルチアプリケーション対応カードの開発が行われている。
【０００３】
また、ＩＣカードのようなセキュリティデバイスをモバイル機器に登載し、アプリケーションのダウンロードやアプリケーション利用を、モバイル機器を介して実施することが実用化されつつある。
【０００４】
ここで、ＩＣカードのハードウェア構成について概観する。
【０００５】
図２６は、ＩＣカードのハードウェアに関する機能ブロック図である。ＩＣカード２６０１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２６０２、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２６０３、揮発性メモリ（例：ＲＡＭ：Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２６０４、揮発性メモリ（例：ＥＥＰＲＯＭ：Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２６０５、Ｉ／Ｏ　ＩＦ２６０６を備えている。ＣＰＵ２６０２は、演算を行う。ＲＯＭ２６０３は書き換えができない読み出し専用のメモリである。ＲＯＭ２６０３に格納される内容は、ＩＣカード製造時に決定され、その後変更することはできない。ＲＡＭ２６０４は読み書きが可能なメモリである。ＥＥＰＲＯＭ２６０５は電源が切断されても内容が保持されるようになっている。Ｉ／Ｏ　ＩＦ２６０６は、ＩＣカードと外部とのデータ交換を担当する。ＣＰＵ２６０２で実行されるプログラムは、通常「アプリケーション」と呼ばれる。アプリケーションの実行のためのコードは、ＲＯＭ２６０３やＥＥＰＲＯＭ２６０５に格納される。また図２６に示す以外に、ＩＣカードが暗号操作のため暗号用コプロセッサを備える場合もある。
【０００６】
ＩＣカードに登載されるアプリケーションと外部（リーダ）は、ＩＳＯ／ＩＥＣ７８１６－４で規定されているＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔ）を使ってデータを交換する。ＡＰＤＵは、リーダがＩＣカードに与えるコマンドと、ＩＣカードからリーダに返すレスポンスの２つの構成からなる。
【０００７】
図２７はＡＰＤＵコマンド２７０１を示しており、ヘッダと本体から構成される。本体は、任意の長さで、空白の場合はなくてもよい。ヘッダは、クラス（ＣＬＡ）、命令（ＩＮＳ）とパラメータ１と２（Ｐ１，Ｐ２）で構成されている。
【０００８】
ＡＰＤＵコマンドはＣＬＡ，ＩＮＳ、Ｐ１，Ｐ２、Ｌｃ　各１バイト、データ部：２５５バイト、Ｌｅ：１バイトの合計２６１バイトが最大であり、アプリケーションをダウンロードするときの数Ｋバイトにおよぶデータを送信するためには、複数のＡＰＤＵブロックにわけて、それぞれのブロックのＰ１やＰ２でブロック番号やあとに続くブロックがあるかとうかを示すことにより、ＩＣカード側で送られてきたコマンドの順番の整合性や最

終処理の必要性をチェックすることができる（図２８参照）。

【０００９】

Ｌｃを３バイトで表記し、１バイト目で３バイト表記であることを示し、２バイト目３バイト目でデータ長を示す拡張が提案されているが、ＩＣカードのメモリ容量の観点から実装例はきわめて少ない。

【００１０】

一般的にＩＣカードのようなメモリ容量の小さなデバイスにおいては、受信したコマンドを格納する入力バッファは大きなサイズを取ることができない。マルチアプリケーション対応カードを用いて説明すると、ある領域を永続的に入力バッファとし、アプリケーション間で共通利用することで確保するメモリ容量を制限している。マルチアプリケーションカードでは、アプリケーションが選択されたときに「現在選択されているアプリケーションを示すカレントＡＰ情報」を更新し、次につづくコマンドを受信したときにカレントＡＰ情報を参照することにより、選択中のアプリケーションに確実にコマンドを渡すことができる。

【００１１】

アプリケーションのダウンロードは、カードマネージャを介して行う。カードマネージャはマルチアプリケーション対応カードにおいてカードの管理やカード内のアプリケーションを管理するアプリケーションである。「カードの管理」とは、カード発行者がカードを管理するために必要なＩＤや鍵をカード内に格納するカード発行や、発行後のカードを一時停止状態や廃棄状態に遷移させることである。また「アプリケーションの管理」とは、アプリケーションのダウンロードや削除をおこなうことである。

【００１２】

また最近では、ＩＣチップから大容量メモリをＩＣカード拡張メモリ保護領域として利用可能なデバイス（以下、セキュアメモリカード）が提案され、ＩＣカードアプリケーションデータの大容量化ニーズに対応可能となる。セキュアメモリカードは、モバイル機器の大きさに適合できることから、スロットつきのモバイル機器に直接挿入し、モバイル機器を利用したＥＣ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｍｍｅｒｃｅ）サービス利用への展開が期待されている。

【００１３】

モバイル機器を利用する場合には、電波圏外に位置することによって通信中断が起こり、その結果としてカードの振る舞いに影響を与える可能性が高くなる。通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理が提案されている。

【特許文献１】特開２００３－１０８３８４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１４】

既存技術においてＩＣカードやセキュアメモリカードなどのセキュアデバイスにアプリケーションをダウンロードする場合に、外部機器側でアプリケーションを複数のＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔ）ブロックに分割して送信する必要がある。セキュアデバイスのメモリ容量増加に伴って高機能アプリケーションが期待され、アプリケーション自体が巨大化する傾向にあり、その結果ＡＰＤＵブロック数はますます多くなる。

【００１５】

モバイル機器を利用する場合には、電波圏外に位置することによって通信中断が起こり、その結果としてカードの振る舞いに影響を与える可能性が高くなる。ＡＰＤＵブロック数の増加はダウンロードが完了するまでに通信中断が発生する可能性が高くなることを意味する。通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理が提案されているが、再送中の失敗による再再送など繰り返し処理によるシステムやカード処理の複雑性、ダウンロード時間の増加によるユーザス

トレスが懸念され、できるだけ通信中断の影響を受けない方式が求められる。

【００１６】

また、カード発行やアプリケーションダウンロードを行う際、種々のセキュリティ対策を行っている。具体的には通信経路上での盗聴を防止し、改竄を検知するためにＡＰＤＵブロックごとに暗号化やＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｅ　Ｃｏｄｅ）付与を行い、カードに送信する。カードでは、ＡＰＤＵブロックの復号化やＭＡＣ検証を実施しているが、カードの処理能力を鑑みると　従来のセキュリティを確保しつつ、すべて平文処理もしくは復号化やＭＡＣ検証の回数を減らすことが可能な方式がのぞましい。

【００１７】

さらに、カード発行やアプリケーションダウンロード時にカードとセッション鍵を共有し、そのセッション鍵でカードに送信するＡＰＤＵブロックの暗号化やＭＡＣを行うためには、元データとなるＡＰＤＵブロックを知る必要がある。

【００１８】

ＡＰＤＵブロック作成者と、カード発行やアプリケーションダウンロードを実行する事業者が分離している場合があり、ＡＰＤＵブロックに個人情報を含む場合にはカード発行やアプリケーションダウンロードを実行する事業者がＡＰＤＵブロックの内容を知ることができない方式が期待されている。

【００１９】

本発明は、こうした従来の問題点を解決するものであり、外部機器とカード間の通信回数を削減し、かつ従来のセキュリティを確保したうえでのカード内セキュリティ処理負荷を軽減することによって外部機器とカード間におけるデータ処理（例：カード発行やアプリケーションダウンロード）の高速化を目的としたものである。

【００２０】

また本発明を利用することよって、カード発行やアプリケーションダウンロードに関与する複数の事業者間において契約によって実現されてきた情報保護を技術的に実現することができる。

【課題を解決するための手段】

【００２１】

本発明のセキュアデバイスは、上記課題を解決するものであり、カード発行のためのコマンド群を保持するコマンド格納部と、前記セキュアデバイスの動作を管理するカード管理部と、外部機器からの指示を受けてコマンド格納部が保持するコマンド群にもとづいて、外部機器からの指示を満たす一連の発行コマンドを選択、構築するカード発行部とを備え、カード発行は、前記カード発行部による前記発行コマンドの出力と前記発行コマンドを受けたカード管理部によるレスポンスからなる、セキュアデバイス内部の通信のみによって実行されるセキュアデバイスである。

【００２２】

コマンド格納部が予めカード発行のためのコマンド群を保持し、カード発行の際はカード内部の通信のみによってカード発行を実現することで、通信中断による発行処理の中断を防ぐとともに、外部機器から受信した信号を復号化するための処理負荷を軽減させることができる。

【００２３】

また、本発明のセキュアデバイスは、外部機器からの指示がカード発行要求かそれ以外かを判別し、カード発行要求の場合は、前記外部機器に発行処理結果を出力することができない特権モードを前記カード管理部に設定する特権モード管理部を備えたものである。

【００２４】

この特権モード管理部により、カード発行中の外部機器からの割り込みや外部機器への誤った出力を防ぐことができる。この場合、発行が終わった後にカードへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除され、以降外部機器からのコマンド送信が可能となる。

【００２５】
また、本発明のセキュアデバイスは、カード発行が成功したことを確認した場合または、カード発行が途中で失敗した場合に、特権モードを解除する特権モード管理部を備えたものである。
【００２６】
この特権モード管理部により、特権モードを解除するために外部機器からのアクションが必要なく、カード発行が終わった直後に外部機器からのコマンドを受信することができる。
【００２７】
また、本発明のセキュアデバイスは、カード発行の進捗状態を逐次、記憶し、前記カード発行の失敗を検出した場合は、失敗を意味する旨と発行処理の進捗状態と、を外部機器に出力することを特徴とするカード管理部を備えたものである。
【００２８】
このカード管理部により、セルフ発行が失敗した場合に外部機器がレスポンスを解析することによって発行がどこまで成功していたかを認識することができる。
【００２９】
また、本発明の外部機器は、発行処理の進捗状態を前記セキュアデバイスから受け取るレスポンス受信部と、発行処理の進捗状態に対応する外部機器の動作を決定するセルフ発行管理部を備えたものである。
【００３０】
カードビジネスでは、カード発行データを準備する事業者と、カード発行を担当する事業者が異なる場合が多い。このセルフ発行管理部により、エラーが発生した場合に実際にカードが処理したコマンドを外部に知られることなく、リカバリ処理が可能となる。
【００３１】
また、本発明のセキュアデバイスは、前記コマンド格納部の発行コマンドを格納する領域を、直接アクセス可能な直接参照手段を更に設け、前記指示がカード発行を意味する場合に、前記カード管理部が、前記直接参照手段を介して前記領域から発行コマンドを取得することを特徴とするものである。
【００３２】
この直接参照手段により、コマンドを分割して処理する場合と比較して、コマンド共通の定型処理や、次のコマンド処理用の準備プロセスを削減し、高速化が可能となる。
【００３３】
また、本発明のセキュアデバイスは、前記カード管理部はカード発行が中断したときの進捗状況をカード発行部に送る中断履歴送信手段を有し、前記カード管理部は、前記中断履歴送信手段から受信した進捗状況をもとに最初に処理するべき発行コマンドを選択、構築するリカバリ手段を有することを特徴とするものである。
【００３４】
中継履歴送信手段とリカバリ手段により、セキュアデバイスへの電源供給が起きたときの進捗状況を意識することなく再試行を実施することができるため、カード発行の負荷が減少する。
【発明の効果】
【００３５】
以上、本発明により、外部機器とカード間の通信回数を削減し、かつ従来のセキュリティを確保したうえでのカード内セキュリティ処理負荷を軽減することによって外部機器とカード間におけるデータ処理（例：カード発行やアプリケーションダウンロード）の高速化を実現することができる。
【発明を実施するための最良の形態】
【００３６】
以下、本発明の実施形態について図を用いて説明する。なお、本発明はこれら実施形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実

施しうる。

【００３７】

以下の実施形態ではセキュアデバイスの例としてマルチアプリケーション対応カードを、発行の例としてアプリケーションダウンロードを採用して説明する。

【００３８】

（実施の形態１）

本実施の形態を図１から図３を用いて説明する。

【００３９】

図１は、本実施の形態におけるセキュアデバイス１０１の構成を示したブロック図である。カード管理部１０２は、外部機器１０５と通信を行い、セキュアデバイス１０１の動作を管理する。カード発行部１０３は、外部機器１０５からの指示を受けて、コマンド格納部１０４が保持するコマンド群にもとづいて、指示を満たす一連の発行コマンドを選択、構築する。コマンド格納部１０４は、カード発行のためのコマンド群を保持する。外部機器１０５は、セキュアデバイスにカード発行用の指示を送出する。

【００４０】

セキュアデバイス１０１は、カード管理部１０２においてアプリケーションが選択されたときに「現在選択されているアプリケーションを示すカレントＡＰ情報」を更新し、次につづくコマンドを受信したときにカレントＡＰ情報を参照することにより、選択中のアプリケーションに確実にコマンドを渡すことができる。

【００４１】

図２は、本実施の形態における外部機器１０５、カード管理部１０２、カード発行部１０３の処理フローを示したものである。

【００４２】

外部機器１０５がカードマネージャを選択するためのコマンドを送信する。カード管理部１０２で選択に成功した場合、現在選択されているＡＰを示す「カレントＡＰ情報」を「カードマネージャ」に更新し、次につづくコマンドを受信したときにカレントＡＰ情報を参照することにより、カードマネージャに確実にコマンドを渡すことができる（ＳＴＥＰ１：アプリケーション選択）。

【００４３】

次に、コマンドを送信する外部機器１０５をセキュアデバイス１０１が認証する外部認証や、外部機器１０５がセキュアデバイス１０１を認証する内部認証を、必要とするセキュリティのレベルに応じて両方、あるいは一方のみ実施する（ＳＴＥＰ２：認証）。

【００４４】

次に、ダウンロードに必要なＡＰＤＵコマンドをまとめたデータ（以下、「連立コマンド」３０１と称する）をコマンド格納部１０４のセキュア領域に書き込む（以下、「ダイレクトアクセス」と称する）。ダイレクトアクセスでは一度に数メガバイトの書き込みが可能であるため、ダウンロードに必要な連立コマンドは通常一回だけのカードアクセスで書き込みが完了する（ＳＴＥＰ３：ダイレクトアクセス）。

【００４５】

連立コマンド３０１の構成を図３に示す。連立コマンド３０１は、いくつのＡＰＤＵコマンド３０４、３０６、３０８、３１０から成り立っているかを示す「ＡＰＤＵ数」３０２と、ＡＰＤＵコマンド３０４、３０６、３０８、３１０が何バイトで構成されているかを示す「コマンド長」３０３、３０５、３０７、３０９と、ＡＰＤＵコマンド３０４、３０６、３０８、３１０からなるデータが複数連なった「コマンド実体部」３１１から成る。それぞれの役割については後述する。

【００４６】

次に外部機器が連立コマンド３０１を利用した発行を開始するための「セルフ発行開始コマンド」を送信する。

【００４７】

図４は、セルフ発行開始コマンド４０１の形式の一例を示した図である。

【００４８】
セルフ発行開始コマンド４０１は、セルフ発行開始コマンドであることを特定するためのヘッダ部４０２と、データ部４０３、４０４、４０５から構成される。
【００４９】
セルフ発行開始コマンドのデータ部４０３、４０４、４０５は、コマンド格納部１０４内に存在する連立コマンド３０１を格納したファイルを特定するためのファイル特定情報（例えばファイル名やファイルＩＤなど）４０３と、特定したファイルからの読み出し位置を示すオフセット４０４、読み出すデータ長４０５から構成される。ただし、連立コマンドを格納するファイルが一意に決まっているなどの理由でデフォルト処理が可能な場合は、ファイル名やファイルＩＤなどを含む必要はない（ＳＴＥＰ４：セルフ発行開始コマンド）。
【００５０】
図５は、セルフ発行開始コマンド４０１を受信してから発行コマンドの読み出しを開始するまでのセキュアデバイス内部の動作フローである。
【００５１】
カード管理部１０２はセルフ発行開始コマンド４０１を受信した後、ヘッダ部４０２を解析してセルフ発行開始コマンドであることを確認する（ＳＴＥＰ５０１）。
【００５２】
次に、カード管理部内に保持するファイル管理テーブル６０１（後述）を参照して、ファイルを特定するための情報４０３に対応するアドレスを特定する（ＳＴＥＰ５０２）。
【００５３】
図６はファイル管理テーブル６０１について示したものである、ファイル管理テーブル６０１は、ファイル名、ファイルのパス、ファイルを特定するための情報、ファイルサイズ、ダイレクトアクセス可能／不可能を示すダイレクトアクセス可能フラグ、アドレスが記述されており、それぞれの内容はファイルを作成したときに追加される。
【００５４】
カード管理部１０２は、発行コマンドを受信した後にレスポンスを送信しない限り、次のコマンドを受信することができない。
【００５５】
ここでは、セルフ発行開始コマンド４０１に対するレスポンスをカード発行部１０３に対して出力する。この場合、セルフ発行開始コマンド４０１に対するレスポンス（以下、セルフ発行トリガと称する）は、カード発行部１０３にとって連立コマンド３０１を処理するためのトリガとなる（ＳＴＥＰ５：セルフ発行トリガ）。
【００５６】
セルフ発行トリガには、アドレス、オフセット４０４、データ長４０５が含まれる。
【００５７】
カード発行部１０３では、アドレスとオフセット４０４から物理的な読み出し位置を特定する（ＳＴＥＰ５０３）。
【００５８】
以後、連立コマンド３０１の読み出しを開始する（ＳＴＥＰ５０４）。読み出し可能な連立コマンド３０１の長さは、セルフ発行開始コマンド４０１に含まれる読み出すデータ長４０５以下でなくてはならない。
【００５９】
カード発行部１０３は、セルフ発行トリガを受け取ると、コマンド長３０３で指定された長さだけ連立コマンド３０１から最初のＡＰＤＵコマンド（例：ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤ）３０４を抽出し、カード発行部内のＡＰＤＵバッファにＡＰＤＵコマンドをコピーする。カード発行部では、ＡＰＤＵコマンドを抽出しＡＰＤＵバッファにコピーするたびごとに、カード発行部で管理する「既出コマンド数」をインクリメントする。既出コマンド数は、セルフ発行トリガを受け取ったときにゼロになっている必要がある。
【００６０】

カード管理部１０２からのレスポンスの送り先はカード発行部１０３となり、ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤが正常終了した場合は、正常終了を意味するステータスワード（例：９０００ｈ）をカード発行部１０３に送る。カード発行部では、ステータスワードが正常終了を意味することを確認し、連立コマンドから次のＡＰＤＵコマンド３０６（例：ＬＯＡＤ１）を抽出し、ＡＰＤＵバッファにＡＰＤＵコマンドをコピーする。以下、既出コマンド数がＡＰＤＵ数と一致するまでこれを繰り返す（ＳＴＥＰ６～ＳＴＥＰｍ：発行コマンド）。

【００６１】

既出コマンド数がＡＰＤＵ数３０２と一致することは、最後の発行コマンド３１０であることを意味する。この場合、カードマネージャが最後のコマンドを正常処理したときのレスポンス送信先は外部機器となる。

【００６２】

またセルフ発行の途中でメモリが枯渇した場合などの異常が発生した場合は、カード発行部１０３が異常を意味するステータスワード（例：6A84h）であることを確認し、異常終了を意味するステータスワードをカード管理部１０２に送信し、カード管理部１０２は異常終了結果をレスポンス（6A84h）として外部機器１０５に送信する。

【００６３】

以上、本実施の形態では、アプリケーションダウンロードにおける外部機器１０５とセキュアデバイス１０１間の通信を、アプリケーションダウンロード時にアプリケーションの大きさに比例して数回～数十回発生していた従来技術と比較して、ダイレクトアクセス（ＳＴＥＰ３）と、セルフ発行開始コマンド（ＳＴＥＰ４）の２回へと減らすことができる。これは、モバイル網利用による通信中断のリスクを大幅に減らすことになる。

【００６４】

さらに、一般的なアプリケーションダウンロードでは、認証時（ＳＴＥＰ２）に外部機器１０５とセキュアデバイス１０１でセッション鍵を共有し、その後外部機器側でＡＰＤＵコマンドに対して暗号化や、改ざんや連続したコマンドであるかを検知するためのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を付与する。外部機器から送られたＡＰＤＵコマンドはカード内で復号やＭＡＣ検証を行っている。

【００６５】

本実施の形態では、外部認証や内部認証によってお互いを認証（ＳＴＥＰ２）したあと、ダイレクトアクセス（ＳＴＥＰ３）によってカード管理部１０２（カードマネージャ）のみがアクセス可能な領域に連立コマンド３０１を格納し、セルフ発行によって外部にデータを出すことなく、すべて耐タンパー性を有するセキュアデバイス内部でダウンロード処理が完結する。したがって、発行時の盗聴や改ざんを考慮する必要がないために暗号化やＭＡＣの付与は必要ない。この結果、カードマネージャは平文を処理するだけでよく、ダウンロード処理が高速になる。

【００６６】

また、送信可能なＡＰＤＵコマンドの全体長が固定であるために、平文の場合は、暗号化やＭＡＣの付与を行ったときに比べて一回のＡＰＤＵコマンドで送信可能なデータが大きい。したがって平文を適用可能な場合は、トータルのコマンド発行数も少なくなり、ダウンロード処理の高速化に有効である。

【００６７】

本実施の形態では、カード交付後にアプリケーションをダウンロードする場合について説明したが、カード交付前に複数アプリケーションのダウンロード用データを格納しておき、ユーザが希望するアプリケーションをセルフ発行することもできる。

【００６８】

（実施の形態２）

本実施の形態２について図７及び８を用いて説明する。

【００６９】

図７は、本実施の形態におけるセキュアデバイス７０１の構成を示したブロック図であ

る。

【００７０】

図７におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外部機器１０５は、それぞれ図１におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外部機器１０５と同様である。

【００７１】

特権モード管理部７０２は、「特権モード」を管理し、カード管理部１０２とカード発行部１０３と連携する。「特権モード」とは、セキュアデバイス内部で連立コマンドを利用したコマンドの送受信を行う（以下、「セルフ発行」と称する。）ためのモードであり、このモードが指定されている間は、セキュアデバイス７０１の接触インタフェースや非接触インタフェースを介して外部機器１０５のやりとりはできない。

【００７２】

図８は、本実施の形態における外部機器１０５、カード管理部１０２、カード発行部１０３、特権モード管理部７０２の処理フローを示したものである。

【００７３】

図８において、ＳＴＥＰ１からＳＴＥＰｍは、実施の形態１で述べた図２と同様である。ＳＴＥＰ５にてカード管理部１０２からセルフ発行トリガをカード発行部１０３が受け取った後に、カード発行部１０３は、特権モード管理部７０２に特権モードへの変更を依頼する（ＳＴＥＰ５－ａ）。あるいは、セルフ発行トリガをカード発行部１０３におくるときに、カード管理部１０２が特権モード管理部７０２に特権モードへの変更を依頼してもよい。

【００７４】

特権モードの間、カード管理部１０２の処理結果（レスポンス）の送り先はカード発行部１０３となり、前述の発行コマンド３０４（ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤ）が正常終了した場合は、正常終了を意味するステータスワード（例：９０００ｈ）をカード発行部１０３に送る。カード発行部１０３では、ステータスワードが正常終了を意味することを確認し、連立コマンド３０１から次のＡＰＤＵコマンド（例：ＬＯＡＤ１）を抽出し、ＡＰＤＵバッファにＡＰＤＵコマンドをコピーする。以下、既出コマンド数がＡＰＤＵ数３０２と一致するまでこれを繰り返す。

【００７５】

既出コマンド数がＡＰＤＵ数３０２と一致することは、最後の発行コマンド３１０であることを意味する。この場合、カード管理部１０２（カードマネージャ）が最後のコマンドを正常処理したときのレスポンス送信先は外部機器１０５となる。

【００７６】

またセルフ発行の途中でメモリが枯渇した場合などの異常が発生した場合は、カード発行部１０３が異常を意味するステータスワードであることを確認し、異常終了を意味するステータスワード（例：6a84hh）をカード管理部１０２に送信し、カード管理部１０２は異常終了結果をレスポンス（6A84h）として外部機器１０５に送信する。

【００７７】

一旦特権モードに遷移すると、セキュアデバイスへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除される。

【００７８】

本実施の形態２では、特権モード管理部７０２にて特権モードに設定されている間は、カード管理部１０２による外部機器１０５からのＡＰＤＵコマンド受信、外部機器１０５へのレスポンス送信を監視することにより、セルフ発行中の外部機器１０５からの割り込みや外部機器１０５への誤った出力を防ぐことができる。この場合、発行が終わった後にセキュアデバイスへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除され、以降外部機器１０５からのコマンド送信が可能となる。

【００７９】
（実施の形態３）
本実施の形態３について図７、図９から図１２を用いて説明する。
【００８０】
本実施の形態３におけるセキュアデバイスの構成は、実施の形態２と同様であり、図７に示したものである。
【００８１】
図９は、本実施の形態における外部機器１０５、カード管理部１０２、カード発行部１０３、特権モード管理部７０１の処理フローを示したものであり、図９においてＳＴＥＰ５－ｂ以外はすべて図８のＳＴＥＰと同様である。
【００８２】
特権モード管理部７０１は、「特権モード」を管理し、カード管理部１０２とカード発行部１０３と連携する。「特権モード」とは、カード内部で連立コマンドを利用したコマンドの送受信を行う（以下、「セルフ発行」と称する。）ためのモードであり、このモードが指定されている間は、セキュアデバイス７０１の接触インタフェースや非接触インタフェースを介して外部機器１０５とのやりとりはできない。
【００８３】
図９において、ＳＴＥＰ１からＳＴＥＰｍは実施の形態１と同様である。ＳＴＥＰ５にてカード管理部１０２からセルフ発行トリガをカード発行部が１０３受け取った後に、カード発行部１０３は、特権モード管理部７０１に特権モードへの変更を依頼する（ＳＴＥＰ５－ａ）。あるいは、セルフ発行トリガをカード発行部１０３におくるときに、カード管理部１０２が特権モード管理部７０１に特権モードへの変更を依頼してもよい。
【００８４】
一旦特権モードに遷移すると、セルフ発行が最後まで正常に終了するか（ＳＴＥＰｍ）途中で失敗したことをカード発行部１０３が認識し、特権モード解除依頼を特権モード管理部７０１に要求するまで特権モードは解除されない（ＳＴＥＰ５－ｂ）。
【００８５】
ここでカード発行部１０３の動作について図１０、図１１を用いて説明する。図１０は、カード発行部１０３がカード管理部１０２からのレスポンスを参照する方式を示した図である。図１１は、カード発行部１０３のレスポンス解析以後の処理フローを示した図である。
【００８６】
まず、カード発行部１０３がカード管理部１０２からレスポンスを受け取った状態になる（ＳＴＥＰ１１０１）。これは、カード管理部１０２で保持するレスポンスバッファに格納されるデータをカード発行部１０３で保持するレスポンスバッファにコピーする方式（図１０（ａ））や、カード管理部１０２で保持するレスポンスバッファに格納されるデータをカード発行部１０３が参照する方式（図１０（ｂ））がある。
【００８７】
この状態はレスポンスの解析が可能な状態であり、レスポンスに含まれるステータスワードを、カード発行部１０３が保持するレスポンス判定テーブル１２０１と比較することによって直前にカード発行部１０３が発行したコマンド処理が成功したか、失敗したかをカード発行部が判断する（ＳＴＥＰ１１０２）。
【００８８】
図１２は、レスポンス判定テーブル１２０１の一例を示した図である。カード発行部１０３は、カード管理部１０２から受け取ったステータスワードとレスポンス判定テーブル１２０１とを対比し、受け取ったステータスワードが９０００ｈであれば、コマンド処理成功と判断し、９０００ｈ以外であれば、コマンド処理失敗と判断する。
【００８９】
成功した場合、発行処理を継続する。失敗した場合、特権モード解除依頼を特権モード管理部７０１に要求し（ＳＴＥＰ１１０３）、レスポンスを外部に送信する（ＳＴＥＰ１

１０４）。

【００９０】

本実施の形態３では、特権モード管理部７０２にて特権モードに設定されている間は、カード管理部１０２が外部機器１０５からＡＰＤＵコマンドを受け取ったり、外部機器１０５にレスポンスを返却したりすることを監視することにより、セルフ発行中の外部機器１０５からの割り込みや外部機器１０５への誤った出力を防ぐことができる。また実施の形態２のように特権モードを解除するために外部機器１０５からのアクションが必要なく、セルフ発行が終わった直後に外部機器１０５からのコマンドを受信することができる。

【００９１】

（実施の形態４）

本実施の形態４について図１３から図１６を用いて説明する。

【００９２】

図１３は本実施の形態におけるセキュアデバイス１３０１の構成を示したブロック図である。カード管理部１０２、カード発行部１０３、コマンド格納部１０４、外部機器１０５はそれぞれ図１で示したものと同様である。

【００９３】

レスポンス演算手段１３０２はカード発行部１０３内に存在し、カード発行の失敗を検出した場合に、失敗を意味する旨と、発行処理の進捗状態を意味するレスポンスデータを作成する手段である。図１４はレスポンス演算手段への入力と出力の関係を示した図である。

【００９４】

実施の形態１において、「カード発行部１０３は、セルフ発行トリガを受け取ると、コマンド長３０３で指定された長さだけ連立コマンド３０１から最初のＡＰＤＵコマンド（例：ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤ）３０４を抽出し、ＡＰＤＵバッファにＡＰＤＵコマンドをコピーする。カード発行部１０３では、ＡＰＤＵコマンドを抽出しＡＰＤＵバッファにコピーするたびごとに、カード発行部１０３で管理する既出コマンド数をインクリメントする。既出コマンド数は、セルフ発行トリガを受け取ったときにゼロになっている必要がある。」と述べた。

【００９５】

また、「またセルフ発行の途中で異常が発生した場合は、カード発行部１０３が異常を意味するステータスワードであることを確認し、異常終了を意味するステータスワードをカード管理部１０２に送信し、カード管理部１０２は異常終了結果を外部機器１０５に送信する。」と述べた。この場合、外部機器１０５はカード管理部１０２から通知される異常終了結果を見てセルフ発行が成功したのか、失敗したのかを判別することができる。

【００９６】

本実施の形態では、セルフ発行が失敗した場合に外部機器１０５が「とこまで成功していたのか」を認識可能な方式について説明する。

【００９７】

図１５は、カード管理部１０２からレスポンスを受け取ったカード発行部１０３のレスポンス解析以後の処理フローを示した図である。ここでＳＴＥＰ１１０１、１１０２、１１０４は実施の形態３で述べたフローと同様である。

【００９８】

カード発行部１０３が異常を意味するステータスワードを、レスポンス判定テーブル１２０１により確認した後（ＳＴＥＰ１１０１、１１０２）、カード発行部７０３はカード発行部１０３内部で保持しているレスポンス演算手段１３０２において、図１４に示すように「既出コマンド数」と異常を意味するステータスワードを入力値として、レスポンスを生成し（ＳＴＥＰ１５０３）、外部機器１０５に出力する（ＳＴＥＰ１１０４）。

【００９９】

レスポンスのフォーマットとしては、２バイトからなるステータスワードのいずれかのビットを利用する場合（例：６３ＣＸｈ（Ｘが既出コマンド数））や、図１６に示すよう

に既出コマンド数（発行処理の進捗状態を示す）をデータ部１６０２に設定し、データ部１６０２とステータスワード（発行処理の失敗した旨を示す）１６０３からなるレスポンス１６０１としてもよい。

【０１００】

本実施の形態では、カード発行部１０３にレスポンス演算手段１３０２を設けることにより、セルフ発行が失敗した場合に外部機器１０５がレスポンス１６０２を解析することによって発行がとこまで成功していたかを認識することができる。

【０１０１】

（実施の形態５）

本実施の形態５について図１６から図１９を用いて説明する。

【０１０２】

図１７は本実施の形態における外部機器１７０１の構成を示したブロック図である。外部機器１７０１は、セルフ発行を制御し、正常か失敗かを判定した後に、該外部機器１７０１の次の動作を決定するセルフ発行管理部１７０２、コマンドを作成するコマンド生成部１７０３、コマンドを送信するコマンド送信部１７０４、レスポンスを受信するレスポンス受信部１７０５から構成される。従来のカード発行では、あらかじめ外部機器が作成した発行コマンドをカードに送信するため、カードから進捗状況を表すレスポンスを受け取る必要はない。外部機器がコマンドを送信し、異常を意味するレスポンスがカードから送られてきたら、異常が発生した原因となるのは直前に送信したコマンドである。

【０１０３】

本実施の形態では、外部機器１７０１は発行要求をセキュアデバイスに送信するのみであるため、セキュアデバイスから発行処理の進捗状態が返却されない限り、とこまでが正常たったかを知ることはできない。

【０１０４】

本実施の形態５では、セルフ発行開始コマンドをセキュアデバイスに送信し、実施の形態４で述べた失敗を意味する旨と発行処理の進捗状態を表すレスポンスをセキュアデバイスから受信した後の外部機器１７０１の挙動について説明する。

【０１０５】

セルフ発行を行う場合、セルフ発行管理部１７０２がコマンド生成部１７０３にセルフ発行開始コマンドの発行を要求する。コマンド作成部１７０３は、コマンド送信部１７０４を介してセキュアデバイスにセルフ発行開始コマンドを送信する。

【０１０６】

図１８は、セキュアデバイスからレスポンスを受信した以後の外部機器１７０１の処理フローを示した図である。なお、レスポンスデータのフォーマットは、実施の形態４で述べた図１６を例として説明する。

【０１０７】

セキュアデバイスからのレスポンスをレスポンス受信部１７０５が受信すると（ＳＴＥＰ１８０１）、セルフ発行管理部１７０２がステータスワードを参照し、例えば９０００ｈであれば成功、それ以外なら失敗と判定する（ＳＴＥＰ１８０２）。

【０１０８】

成功の場合、セルフ発行処理を終了する。また、セルフ発行は成功したが確認用のコマンドを外部機器１７０１から受け取った後に使用可能となる場合は、コマンド生成部１７０３に「カード使用許可確認用コマンド」を発行するように要求する。

【０１０９】

あるいは、外部機器１７０１にインターネット接続やモバイル通信用のインタフェースを設け、成功した結果を、別の外部機器に通知することもある。

【０１１０】

ステータスワードが失敗の場合、セルフ発行管理部１７０２は、レスポンスに含まれる既出コマンド数をキーにして、セルフ発行管理部１７０２が保持する進捗管理テーブル１９０１を参照する（ＳＴＥＰ１８０３）。

【０１１１】
図１９は、進捗管理テーブル１９０１の一例を示した図であり、セキュアデバイスから受け取ったレスポンスに含まれる「既出コマンド数」と、その「既出コマンド数」に対応する外部機器１７０１の処理内容が、「既出コマンド数」毎に記載されている。
【０１１２】
セルフ発行管理部１７０２は、セキュアデバイスから受け取ったレスポンスに含まれる「既出コマンド数」を抽出し、進捗管理テーブル１９０１を参照して、次の動作を決定する。
【０１１３】
レスポンス１６０１の既出コマンド数がｎの場合には、進捗管理テーブル１９０１に従ってコマンド生成部１７０３に、発行中に書き込んだデータをすべてクリアするための「クリアコマンド」を要求する（ＳＴＥＰ１８０４）。
【０１１４】
コマンド生成部１７０３は、従来のカード発行において外部機器がカードに送信する鍵やＩＤを設定するコマンドや、アプリケーション用のデータを設定するコマンドではなく、セルフ発行開始コマンドと、クリアコマンドやカード使用許可確認コマンドのような、セキュリティ保護が必要ない発行後処理コマンドを作成する。
【０１１５】
カードビジネスでは、カード発行データを準備する事業者と、カード発行を担当する事業者が異なることがある。
【０１１６】
提案する方式に適用すると、カード発行データを準備する事業者は図２、図８、図９においてＳＴＥＰ３まで、カード発行を担当する事業者はステップ４以降を実施することになる。
【０１１７】
一般的に外部機器１７０１を用いてカード発行を担当する事業者は、とのようなカード発行データを用いてカード発行を実施しているかを知らないほうがセキュリティの観点で望ましい。
【０１１８】
本実施の形態では、とのようなコマンドを発行したかをカード発行担当事業者が知ることなく発行が完了するために、セキュリティ保護を実現できる。
【０１１９】
（実施の形態６）
本実施の形態を図２０、図２１、図３を用いて説明する。
【０１２０】
図２０は、本実施の形態におけるセキュアデバイス２００１の構成を示したブロック図である。
【０１２１】
図２０におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外部機器１０５は、それぞれ図１におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外部機器１０５と同様である。２００２はカード管理部に含まれ、コマンド格納するＡＰＤＵバッファ、２００３は連立コマンドが格納された領域を、直接アクセス可能な直接参照手段である。２００４は、コマンド格納部１０４の連立コマンドが格納された領域の一部を、連立コマンドのＡＰＤＵバッファとして、一時的に利用される連立コマンドＡＰＤＵバッファである。直接参照手段２００３は、この連立コマンドＡＰＤＵバッファ２００４を、直接参照することができる。
【０１２２】
図２１は、本実施の形態における連立コマンドを示す。
【０１２３】
連立コマンド２１０１は、いくつのＡＰＤＵコマンド２１０４、２１０６から成り立っ

ているかを示すＡＰＤＵ数２１０２と、ＡＰＤＵコマンド２１０４、２１０６が何バイトで構成されているかを示す、コマンド長２１０３、２１０５と、ＡＰＤＵコマンド２１０４、２１０６からなるデータが複数連なった、コマンド実体部２１１１から成る。それぞれの役割については後述する。

【０１２４】

本実施の形態１から４では、セルフ発行開始コマンドにてカード発行部が連立コマンドを格納するファイルを特定し、ファイルに含まれるＡＰＤＵコマンドを抽出して、一旦、カード管理部１０２内のＡＰＤＵバッファにコピーすることによってカード管理部（カードマネージャはカード管理部の一部となる）は、ＡＰＤＵコマンドが外部機器から接触インタフェースや非接触インタフェースを介して送られてきたものか、セルフ発行によるものか、を区別することなくＡＰＤＵコマンドを実行する方法を述べた。

【０１２５】

本実施の形態６では、接触インタフェースや非接触インタフェースを利用する際のＡＰＤＵバッファ２００２と、セルフ発行時のＡＰＤＵを格納するバッファとを共有しない形態について説明する。

【０１２６】

実施の形態１と同様にセルフ発行開始コマンドに対するレスポンス（以下、セルフ発行トリガと称する。）は、カード発行部１０３にとって連立コマンド２１０１を処理するためのトリガとなる。

【０１２７】

カード発行部１０３はセルフ発行トリガを受け取るとコマンド長２１０３で指定された長さだけ連立コマンド２１０１から最初のＡＰＤＵコマンド（例：ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤ）２１０４を抽出し、コマンド格納部１０４内にＡＰＤＵコマンド長さ分の領域をＡＰＤＵバッファとして指定する。

【０１２８】

このとき、外部機器１０５からのＡＰＤＵコマンドを格納するＡＰＤＵバッファ２００２と連立コマンド用のＡＰＤＵバッファ２００４が並存する。すなわち外部機器１０５からのＡＰＤＵコマンドを格納するＡＰＤＵバッファ２００２はカード管理部に属し、連立コマンド用のＡＰＤＵバッファ２００４はコマンド格納部１０４に属する。

【０１２９】

例えば最初のＡＰＤＵコマンド（ＩＮＳＴＡＬＬ　ＦＯＲ　ＬＯＡＤ）を処理する場合には、ＡＰＤＵコマンド２１０４で表す発行コマンド１－ａが占める領域自体が連立コマンド用ＡＰＤＵバッファとなる。

【０１３０】

外部機器１０５からのＡＰＤＵコマンドを格納するＡＰＤＵバッファ２００２が固定領域として永続するのに対して、連立コマンド用のＡＰＤＵバッファ２００４は、あるコマンドを処理する瞬間のみ、そのコマンドが入っている領域を占めるものであり、次のコマンドを処理するごとに時々刻々と領域のアドレスや大きさが変化する。すなわち、発行コマンド１が処理されたら次は、発行コマンド２－ａが占める領域自体が連立コマンド用ＡＰＤＵバッファとなる。

【０１３１】

ここで実施の形態１における連立コマンドを示す図３と本実施の形態における連立コマンドを示す図２１を比較する。図３においてＬＯＡＤコマンドは発行コマンド２から発行コマンドｍに分割されている。例えばダウンロード対象のデータが２０００キロバイトであった場合、一回で送信可能な、つまりＡＰＤＵバッファ２００２に格納可能なデータ長の最大が２５５バイトとすると（ただし平文の場合。暗号化やＭＡＣ付与の場合はより短くなる。）、２５５×７＜２０００＜２５５×８となり８コマンドに分割して送る必要があるため、ｍ＝９となる。

【０１３２】

これに対し、図２１においては、ＬＯＡＤコマンドを連立コマンド用ＡＰＤＵバッファ

２００４で指定することで、一回の処理で完結させることができる。

【０１３３】

カードマネージャは、カード管理部１０２のＡＰＤＵバッファ２００２からデータを取得する場合と同様に、直接参照手段２００３を介することで連立コマンド用ＡＰＤＵバッファ２００４からデータを取得する。いずれの場合もカードマネージャの挙動としては、ＡＰＤＵバッファにアクセスする点で等価な処理となる。

【０１３４】

直接参照手段２００３を利用するタイミングは、セルフ発行開始コマンドを受信した後にカード管理部１０２から直接参照手段２００３に要求する場合や、カード発行部１０３がセルフ発行トリガを受け取って、直接参照手段２００３に要求してもよい。

【０１３５】

なお、特権モード管理部７０２を設けて、特権モードのときだけこの直接参照手段２００３を利用可能としてもよい。

【０１３６】

次に、実施の形態１の場合のように複数回にわけてＬＯＡＤコマンドを受信する場合と、本実施の形態の場合のように一回でＬＯＡＤコマンドを受信する場合のカードマネージャの動作を説明する。

【０１３７】

複数回にわけてＬＯＡＤコマンドを処理する場合、コマンド数分、ＡＰＤＵコマンド受信処理、ＡＰＤＵバッファからのデータ取得処理、そのコマンドが正しい順番で送られてきているか、最後のコマンドであるかのコマンドチェック、データの処理、次のコマンドを処理するための中間状態の保持、レスポンス送信処理が必要となる。

【０１３８】

一方、ＬＯＡＤコマンドを一回で処理する場合、ＡＰＤＵコマンド受信処理、ＡＰＤＵバッファからのデータ取得処理、コマンドチェック、レスポンス送信処理が一回だけとなり、また次のコマンドを処理するための中間状態の保持はいらない。

【０１３９】

このように、本実施の形態では直接参照手段２００３を備えることで、コマンドを分割して処理する場合と比較して、コマンドごとに行う必要のある定型処理を大幅に減らし、また次のコマンドに備えるための冗長な処理をなくすことができる。この結果として、外部機器からＡＰＤＵを複数回にわけてダウンロードする従来のやり方に対して、大幅な高速化が可能となる。

【０１４０】

読み／書き機能を有する携帯電話等の可搬性の高いモバイル端末を用いてセキュアデバイスにアプリケーションをダウンロードする場合、一般的に電源となる電池容量が有限であることから高速化の意義は大きい。

【０１４１】

さらには、セキュアデバイスが携帯電話に抜き差しできるリムーマブルメディアの場合、ユーザが突然電源を切るケースやダウンロード処理途中にセキュアデバイスを抜くことによるセキュアデバイスへの電源供給停止が起こりうる。これらのケースにおいても、高速処理できることはユーザの誤った操作の影響をうける可能性が小さくなることを意味するため意義は大きい。

【０１４２】

（実施の形態７）

本実施の形態を図２２から図２４を用いて説明する。

【０１４３】

図２２は、本実施の形態におけるセキュアデバイス２２０１の構成を示したブロック図である。

【０１４４】

図２２におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外

部機器１０５は、それぞれ図１におけるカード管理部１０２，カード発行部１０３，コマンド格納部１０４，外部機器１０５と同様である。２２０２は実施の形態１から６で説明した既出コマンド数を保持し、カード発行部１０３に送信する中断履歴送信手段、２２０３は中断履歴送信手段から受信した既出コマンド数に応じたリカバリを実施するリカバリ手段である。

【０１４５】

図２３は本実施の形態における連立コマンドを示す。

【０１４６】

図２３における３０２～３１１は、図３における３０２～３１１と同様である。

【０１４７】

連立コマンド２３０１は、図３で示した、いくつのＡＰＤＵコマンド３０４、３０６、３０８、３１０から成り立っているかを示す「ＡＰＤＵ数」３０２と、リカバリを実施する際に参照するリカバリ情報２３０２と、ＡＰＤＵコマンド３０４、３０６、３０８、３１０がそれぞれ何バイトで構成されているかを示す「コマンド長」３０３、３０５、３０７、３０９と、発行コマンド３０４、３０６、３０８、３１０からなるデータが複数連なった「コマンド実体部」３１１とから成る。

【０１４８】

図２５は、リカバリ情報２３０２の一例を示した図である。リカバリ情報２３０２は、リカバリ情報の長さを表すリカバリ情報長２４０１と、リカバリ時にどのコマンドから発行するかを示すコマンド番号２４０２、２４０４と、コマンド番号で特定される発行コマンドが連立コマンド１３０２のどの位置から始まっているかを表すオフセット２４０３、２４０５から構成される。なお、コマンド番号２４０２，２４０４とオフセット２４０３、２４０５は組となって複数設定することができる。

【０１４９】

カード発行途中にカードへの電源供給がなくなる（以下、電源断）とカードは処理を中止し、レスポンスを外部機器１０５に送信することはない。実施の形態１～６で述べてきたセルフ発行においてレスポンスが外部機器１０５に到達しないことは、電源断が生じたとき即座にカード発行の進捗状況を外部機器が知ることができないことを意味する。

【０１５０】

なお、電源断の検知については、例えば、セッションタイムアウトを利用することによって可能である。

【０１５１】

本実施の形態では、電源断を検知後、セキュアデバイス２２０１のリカバリ処理を実施について説明する。

【０１５２】

リカバリ処理は以下の３パターンに区分されるカード実装に依存する。

【０１５３】

７－１）電源断発生後に、電源供給が発生したときや、最初のコマンドを受け取ったときに、電源断が生じるまでにセキュアデバイス２２０１内で確保した領域や格納したデータをすべてクリアする場合

この場合のリカバリ処理は、カード発行を最初からやり直すことになる。このような実装を施したセキュアデバイス２２０１は、カード管理部１０２が管理する既出コマンド数はＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）などの一次記憶領域に保持しておけばよい。

【０１５４】

外部機器１０５も電源断を検知した後に発行が要求されたときにセルフ発行開始コマンドを送信すればよい。

【０１５５】

７－２）それまでに確保した領域や格納したデータはそのままで、電源断がおきたコマンドからやり直しができる場合（コマンド単位でリカバリ処理可能な場合）

この場合のリカバリ処理は、電源断がおきたコマンドからやり直すことになる。このような実装を施したセキュアデバイス２２０１では、電源断が発生した前回の処理において何番目のコマンドで失敗したかを記憶しておく必要がある。

【０１５６】

したがってカード管理部１０２が管理する既出コマンド数は、ＥＥＰＲＯＭなどの不揮発性記憶領域に保持する必要がある。

【０１５７】

図２５は、セキュアデバイス２２０１におけるリカバリ処理の動作を示したフロー図である。

【０１５８】

電源断発生後に外部機器１０５からセルフ発行コマンドが送信された場合、カード管理部１０２はセルフ発行コマンドであることを確認した後（ＳＴＥＰ２５０１）、既出コマンド数がゼロでないことを確認する（ＳＴＥＰ２５０２）。ここで既出コマンド数がゼロでないことは、前回の発行が電源断によって中断されたことを意味する。

【０１５９】

次に、カード管理部１０２は既出コマンド数を中断履歴送信手段２２０２を介してカード発行部１０３に渡す（ＳＴＥＰ２５０３）。カード発行部１０３では、リカバリ手段２２０３が連立コマンド２３０１の一部であるリカバリ情報２３０２を検索し、既出コマンド数と一致するコマンド番号２４０２、２４０４を検索し、該当するコマンド番号が存在した場合にコマンド番号と対になる先頭からのオフセット２４０３、２４０５を抽出することで今回最初に送るべきコマンドを特定する（ＳＴＥＰ２５０４）。次に、特定したコマンドを読み出し、カード管理部のＡＰＤＵバッファにコピーし発行が再開される（ＳＴＥＰ２５０５）。

【０１６０】

本方式ではリカバリ情報２３０２を参照することで読み出し位置を決定する内容について述べたが、リカバリ情報２３０２を付与せず図３で述べた連立コマンド３０１を先頭から解析することで読み出し位置を特定してもよい。たとえば、既出コマンド数が２であれば、コマンド長３０３が存在するアドレスを特定し、指定された長さをアドレスに加えて、コマンド長３０５が存在するアドレスを特定し、その後に続く発行コマンド２（Ｌｏａｄ１）３０６の読み出し位置が決定されることになる。

【０１６１】

７－３）それまでに確保した領域や格納したデータはそのまま、あるいは「あるコマンド」処理以前に確保した領域や格納したデータがそのままで、「あるコマンド」以降からやり直しができる場合（機能単位でリカバリ処理）

図２４において、コマンド番号１（２４０２）に「１」、コマンド番号２（２４０４）に「２」が設定されているとする。

【０１６２】

発行コマンド３（Ｌｏａｄ２）３０８は３番目のコマンドであり、ここで電源断が発生した場合、カード管理部１０２が管理する既出コマンド数は「３」のままＥＥＰＲＯＭなどの不揮発性記憶領域に保持されている。

【０１６３】

図２５は、セキュアデバイス２２０１におけるリカバリ処理の動作を示したフロー図である。

【０１６４】

外部機器１０５からセルフ発行開始コマンドが送信された場合、カード管理部１０２はセルフ発行コマンドであることを確認した後（ＳＴＥＰ２５０１）、既出コマンド数がゼロでないことを確認する（ＳＴＥＰ２５０２）。ここで既出コマンド数がゼロでないことは、前回の発行が電源断によって中断されたことを意味する。

【０１６５】

次に、カード管理部１０２は既出コマンド数「３」を中断履歴送信手段２２０２を介し

てカード発行部１０３に渡す（ＳＴＥＰ２５０３）。

【０１６６】

カード発行部１０３のリカバリ手段２２０３では、既出コマンド数「３」とコマンド番号１（１４０２）に設定されている「１」、コマンド番号２（１４０４）に設定されている「２」と比較して、１＜２＜３の関係になることから、「３」より小さく、「３」に最も近い「２」からやり直すことを決定する（ＳＴＥＰ２５０４）。

【０１６７】

次に、カード発行部１０３はコマンド番号２に該当する発行コマンド２（Ｌｏａｄ１）３０６を抽出してＡＰＤＵバッファにコピーし発行が再開される（ＳＴＥＰ２５０５）。

【０１６８】

本実施の形態では、カード管理部１０２に中断履歴送信手段２２０２、カード発行部１０３にリカバリ手段２２０３を備えることで、カード発行途中にカードへの電源供給がなくなった場合の事後処理において再試行が可能となる。

【０１６９】

外部機器１０５は、カードへの電源供給が起きたときの進捗状況を意識することなく再試行を実施することができるため、カード発行の負荷が減少する。

【産業上の利用可能性】

【０１７０】

本発明のセキュアデバイスと外部機器は、外部機器からセキュアデバイスへ１度の指示を出すことにより、後はセキュアデバイス内で自立的に処理を実行することができので、カードとの間の通信状態が不良の下でのカード発行や、ユーザが持っている携帯端末機器を利用して個人が自由にカード発行することに適している。

【図面の簡単な説明】

【０１７１】

【図１】本発明の実施の形態１におけるセキュアデバイスのブロック図

【図２】本実施の形態１における処理フロー図

【図３】連立コマンドの一例を示す図

【図４】セルフ発行開始コマンドフォーマットの一例を示す図

【図５】セルフ発行コマンドを受信してから発行コマンドの読み出しを開始するまでのセキュアデバイス内部の動作フロー図

【図６】ファイル管理テーブルの一例を示す図

【図７】本発明の実施の形態２、３におけるセキュアデバイスのブロック図

【図８】本実施の形態２における処理フロー図

【図９】本実施の形態３における処理フロー図

【図１０】カード発行部がカード管理部からのレスポンスを参照する方式例を示す図

【図１１】レスポンス解析以後の処理フロー図

【図１２】レスポンス解析用の参照テーブルの一例を示す図

【図１３】本発明の実施の形態４におけるセキュアデバイスのブロック図

【図１４】レスポンス演算手段への入力と出力の関係図

【図１５】レスポンス解析以後の処理フロー図

【図１６】レスポンスデータフォーマットの一例を示す図

【図１７】本実施の形態５における外部機器の構成を示したブロック図

【図１８】レスポンスを受信した以後の外部機器における処理フロー図

【図１９】セルフ発行管理部が次の動作を決定するための進捗管理テーブルの一例を示す図

【図２０】本実施の形態６におけるセキュアデバイスの構成を示したブロック図

【図２１】本実施の形態６における連立コマンドの一例を示す図

【図２２】レスポンスデータフォーマットの一例を示す図

【図２３】本実施の形態７における連立コマンドの一例を示す図

【図２４】リカバリ情報の一例を示す図

【図２５】リカバリを実施するときの処理フロー図
【図２６】ＩＣカードのハードウェアに関する機能ブロック図
【図２７】ＡＰＤＵコマンドのフォーマット図
【図２８】データを分割してＡＰＤＵを作成する方式の概念図

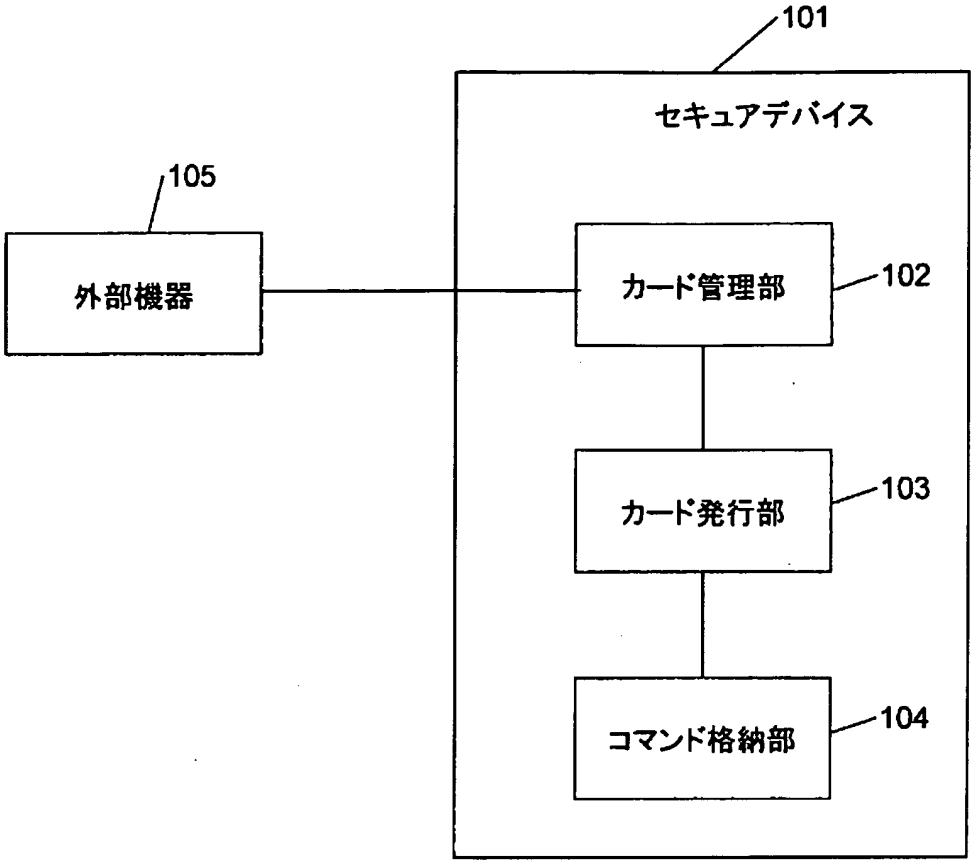
【符号の説明】

【０１７２】

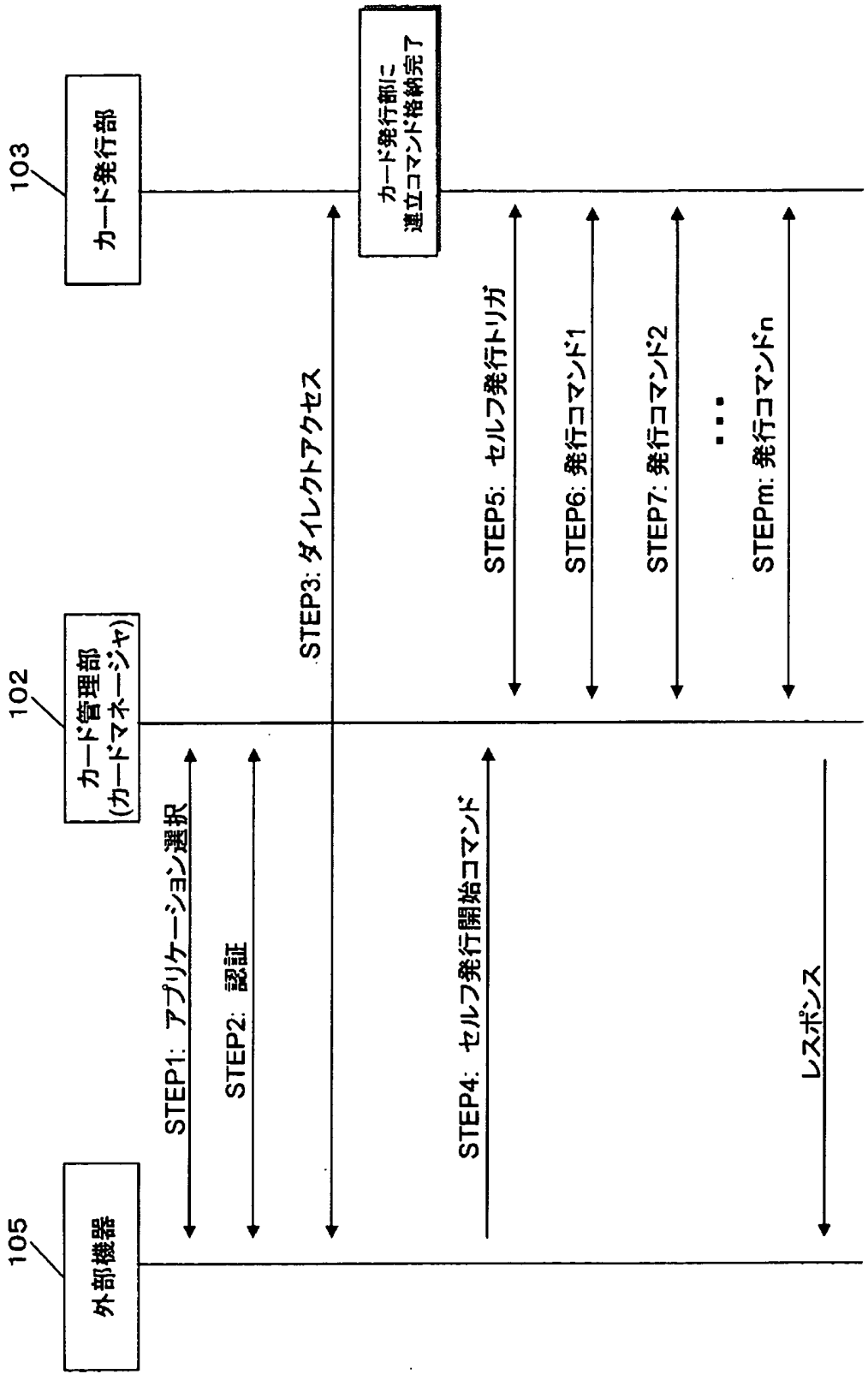
１０１　セキュアデバイス
１０２　カード管理部
１０３　カード発行部
１０４　コマンド格納部
１０５　外部機器
３０１　連立コマンド
３０２　ＡＰＤＵ数
３０３，３０５，３０７，３０９　コマンド長
３０４，３０６，３０８，３１０　発行コマンド
３１１　コマンド実体部
４０１　セルフ発行コマンド
４０２　ヘッダ部
４０３　ファイル特定情報
４０４　ファイルからの読み出し位置（オフセット）
４０５　読み出すデータ長
６０１　ファイル管理テーブル
７０１　セキュアデバイス
７０２　特権モード管理部
１２０１　レスポンス解析用参照テーブル
１３０１　セキュアデバイス
１３０２　レスポンス演算手段
１６０１　レスポンス
１６０２　データ部
１６０３　ステータスワード
１７０１　外部機器
１７０２　セルフ発行管理部
１７０３　コマンド生成部
１７０４　コマンド送信部
１７０５　レスポンス受信部
１９０１　進捗管理テーブル
２００１　セキュアデバイス
２００２　ＡＰＤＵバッファ
２００３　直接参照手段
２００４　連立コマンド用ＡＰＤＵバッファ
２１０１　連立コマンド
２１０２　ＡＰＤＵ数
２１０３，２１０５　コマンド長
２１０４，２１０６　発行コマンド
２１１１　コマンド実体部
２２０１　セキュアデバイス
２２０２　中断履歴送信手段
２２０３　リカバリ手段
２３０１　連立コマンド
２３０２　リカバリ情報

２４０１　　リカバリ情報長
２４０２，２４０４　　コマンド番号
２４０３，２４０５　　オフセット
２６０１　　ＩＣカード
２６０２　　ＣＰＵ
２６０３　　ＲＯＭ
２６０４　　ＲＡＭ
２６０５　　ＥＥＰＲＯＭ
２６０６　　Ｉ／Ｏ　ＩＦ
２７０１　　ＡＰＤＵコマンド

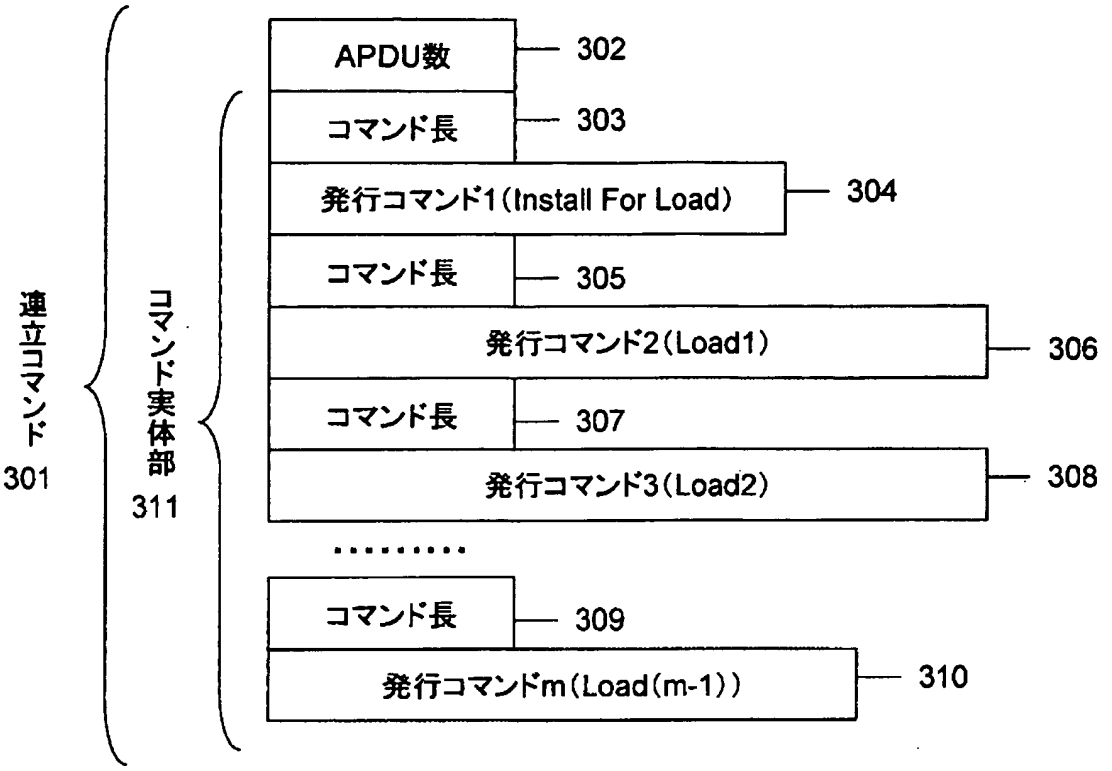
【書類名】図面
【図１】



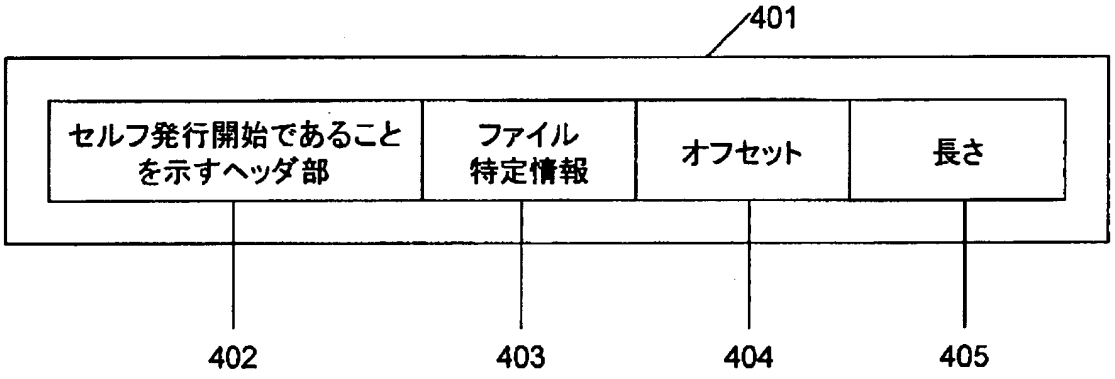
【図２】


103
カード発行部
カード発行部に
連立コマンド格納完了
102
カード管理部
(カードマネージャ)
STEP1: アプリケーション選択
STEP2: 認証
STEP3: ダイレクトアクセス
STEP4: セルフ発行開始コマンド
STEP5: セルフ発行トリガ
STEP6: 発行コマンド1
STEP7: 発行コマンド2
・・・
STEPm: 発行コマンドn
レスポンス
105
外部機器

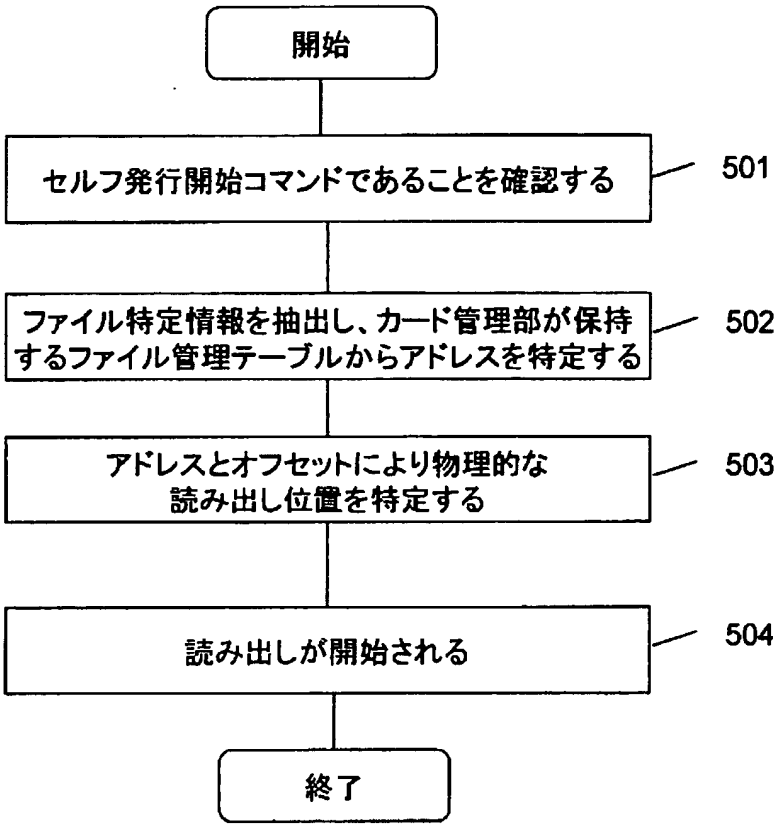
【図３】


連立コマンド
301
コマンド実体部
311
APDU数
302
コマンド長
303
発行コマンド1(Install For Load)
304
コマンド長
305
発行コマンド2(Load1)
306
コマンド長
307
発行コマンド3(Load2)
308
.....
コマンド長
309
発行コマンドm(Load(m-1))
310

【図４】


401
セルフ発行開始であること
を示すヘッダ部
ファイル
特定情報
オフセット
長さ
402
403
404
405

【図５】

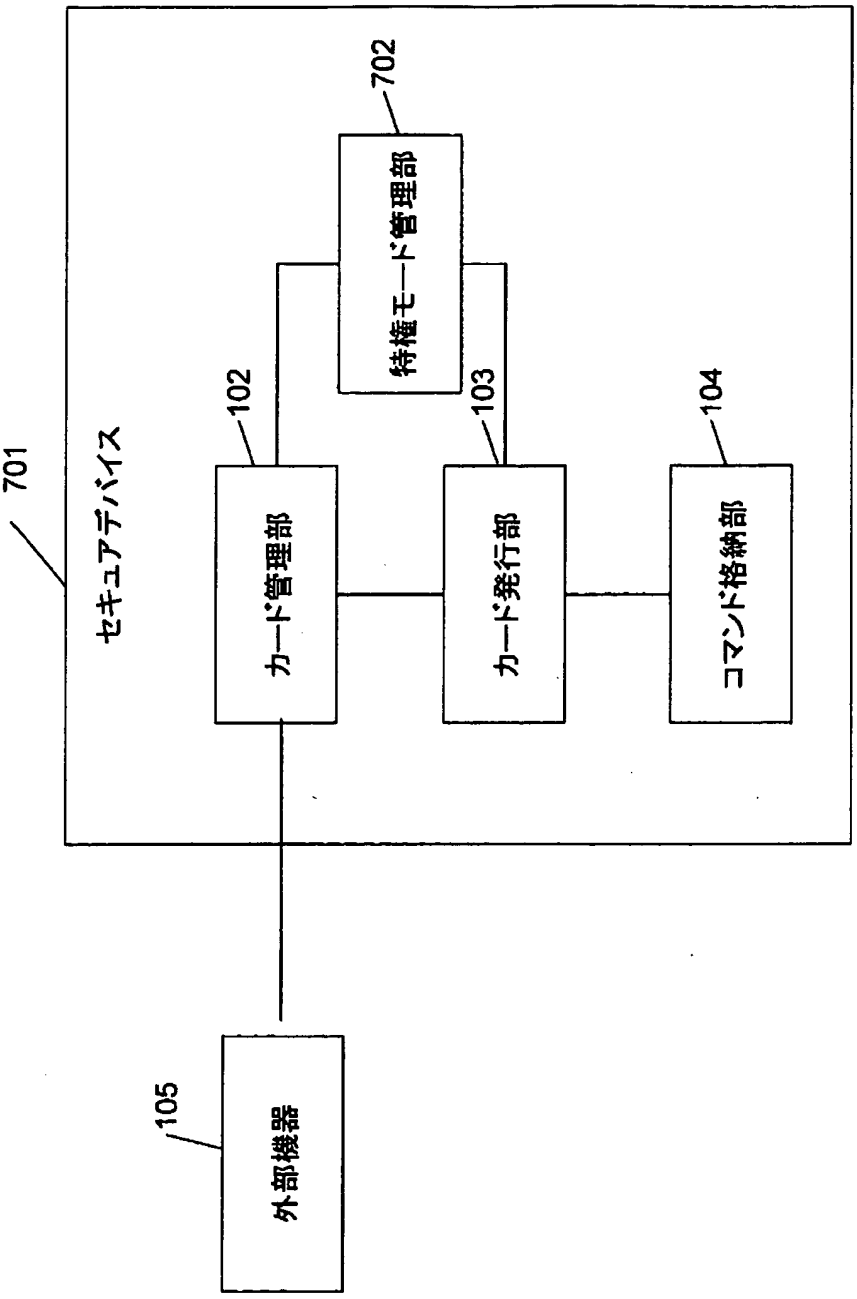

開始
セルフ発行開始コマンドであることを確認する
501
ファイル特定情報を抽出し、カード管理部が保持するファイル管理テーブルからアドレスを特定する
502
アドレスとオフセットにより物理的な読み出し位置を特定する
503
読み出しが開始される
504
終了

【図６】

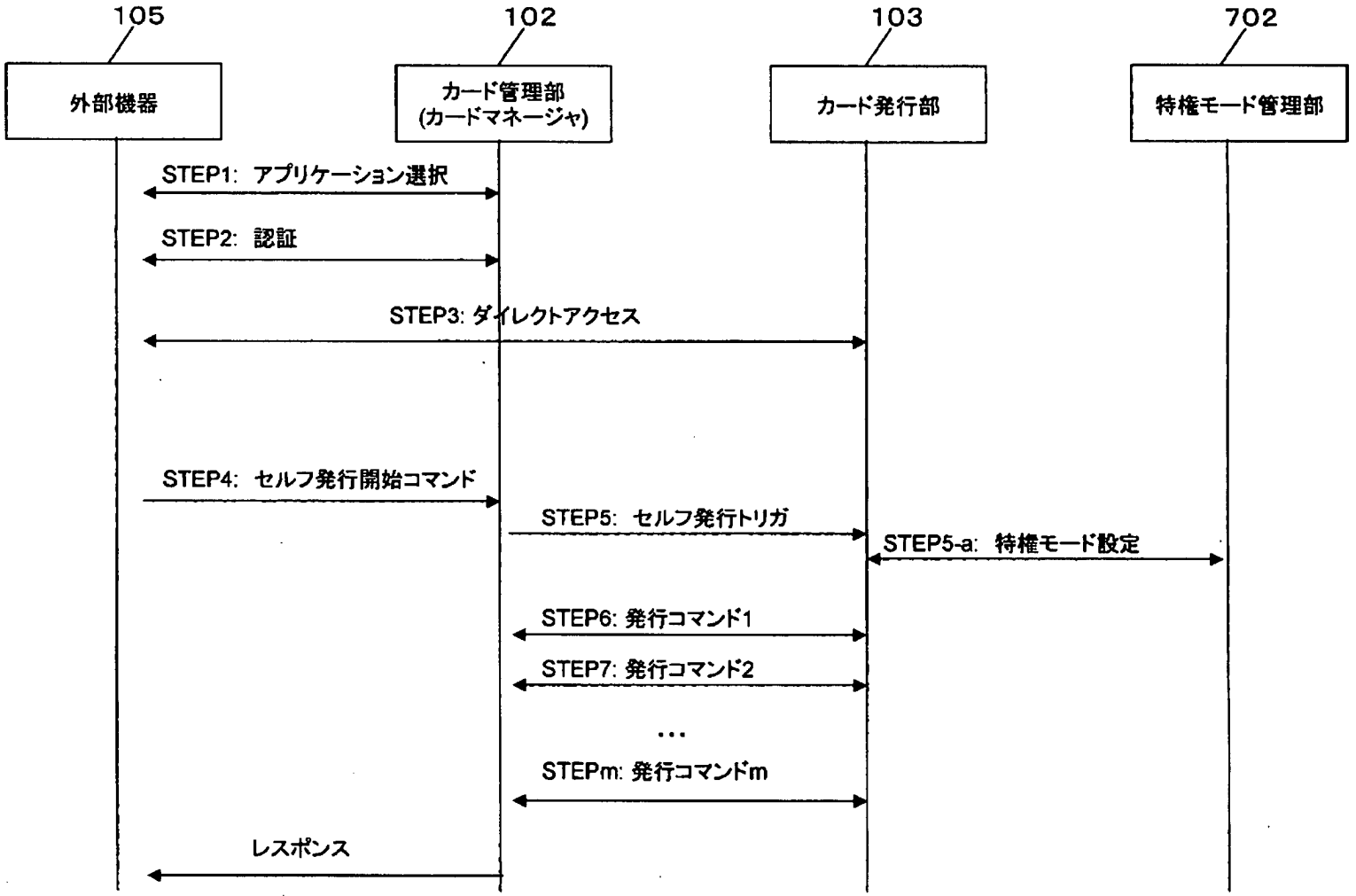
601

ファイル名	ファイルパス	ファイル特定情報	ファイルサイズ	ダイレクトアクセス可能フラグ	アドレス
File_1	Root/	1	a	true	＊＊＊＊
File_2	Root/dir1	2	b	true	△△ △△

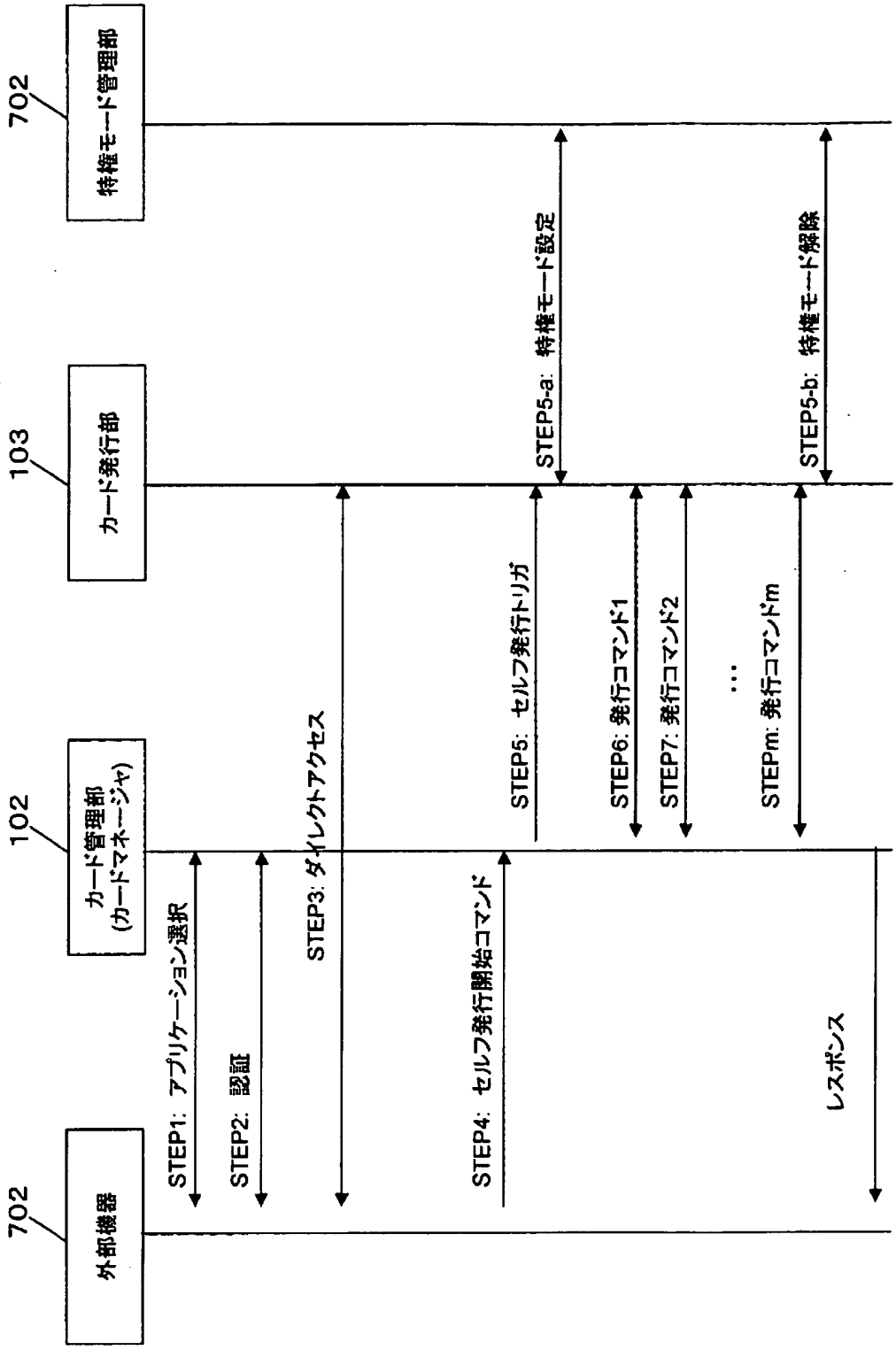
【図７】


701
セキュアデバイス
702
特権モード管理部
102
カード管理部
103
カード発行部
104
コマンド格納部
105
外部機器

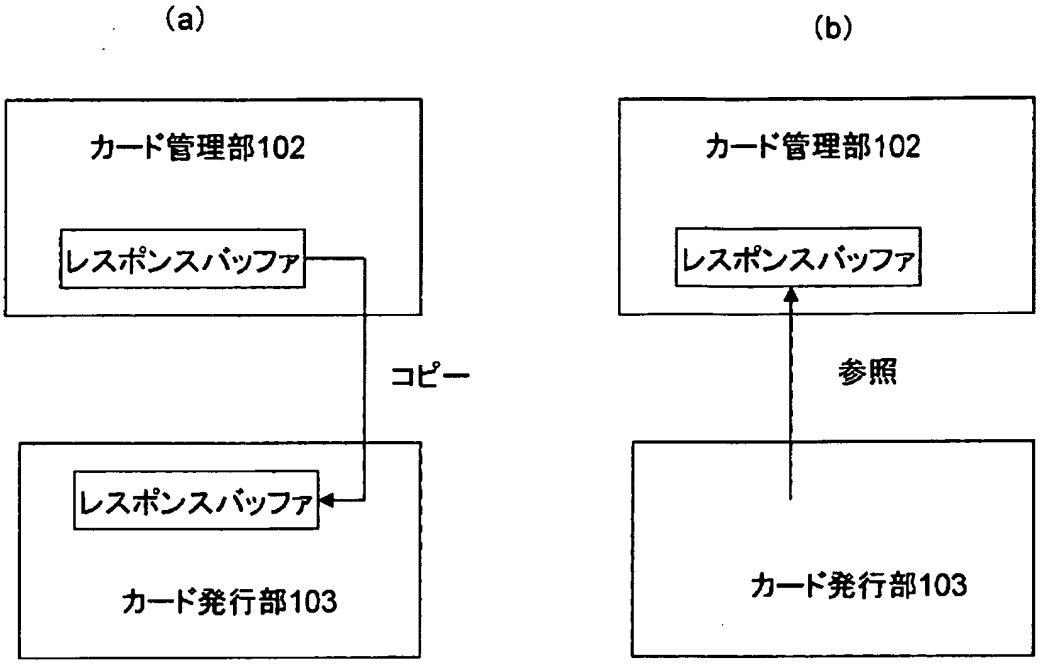
【図８】


105
102
103
702
外部機器
カード管理部
(カードマネージャ)
カード発行部
特権モード管理部
STEP1: アプリケーション選択
STEP2: 認証
STEP3: ダイレクトアクセス
STEP4: セルフ発行開始コマンド
STEP5: セルフ発行トリガ
STEP5-a: 特権モード設定
STEP6: 発行コマンド1
STEP7: 発行コマンド2
...
STEPm: 発行コマンドm
レスポンス

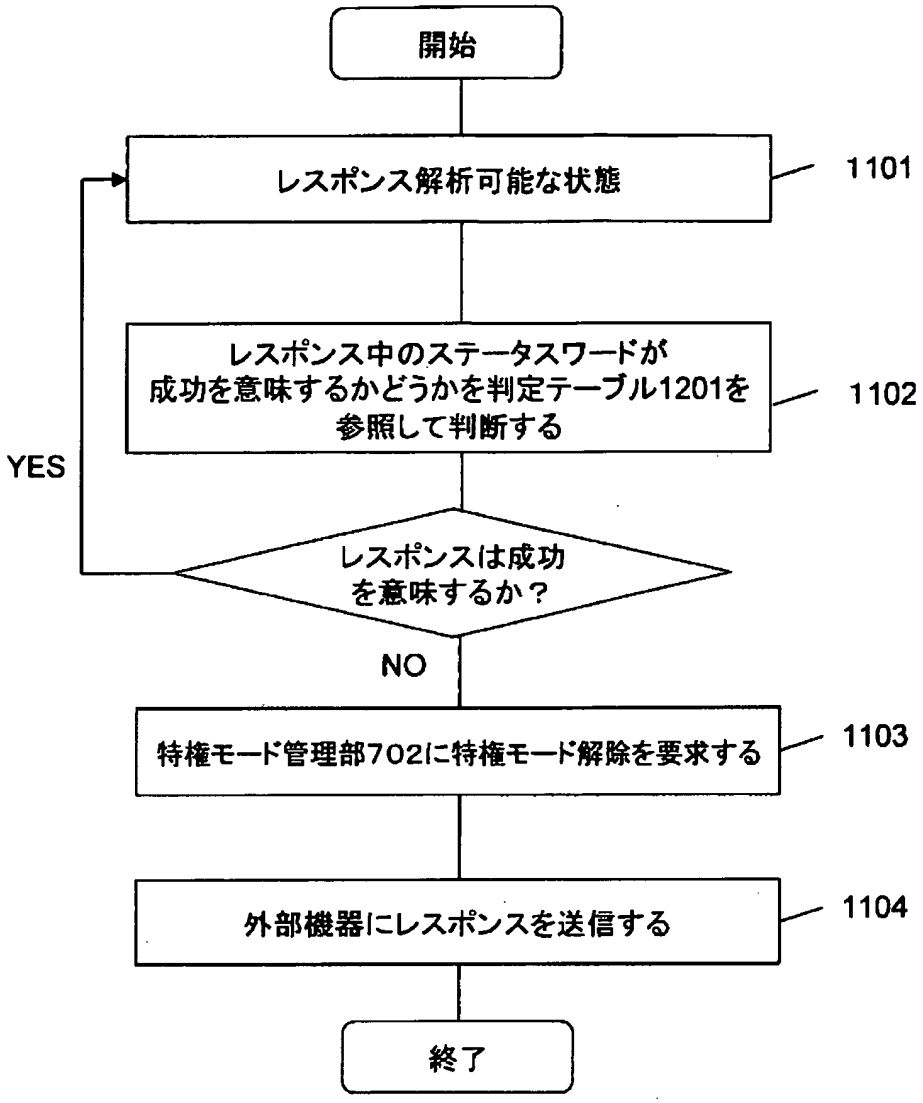
【図９】


外部機器
702
カード管理部
(カードマネージャ)
102
カード発行部
103
特権モード管理部
702
STEP1: アプリケーション選択
STEP2: 認証
STEP3: ダイレクトアクセス
STEP4: セルフ発行開始コマンド
STEP5: セルフ発行トリガ
STEP5-a: 特権モード設定
STEP6: 発行コマンド1
STEP7: 発行コマンド2
...
STEPm: 発行コマンドm
STEP5-b: 特権モード解除
レスポンス

【図１０】


(a)
(b)
カード管理部102
レスポンスバッファ
コピー
レスポンスバッファ
カード発行部103
カード管理部102
レスポンスバッファ
参照
カード発行部103

【図１１】

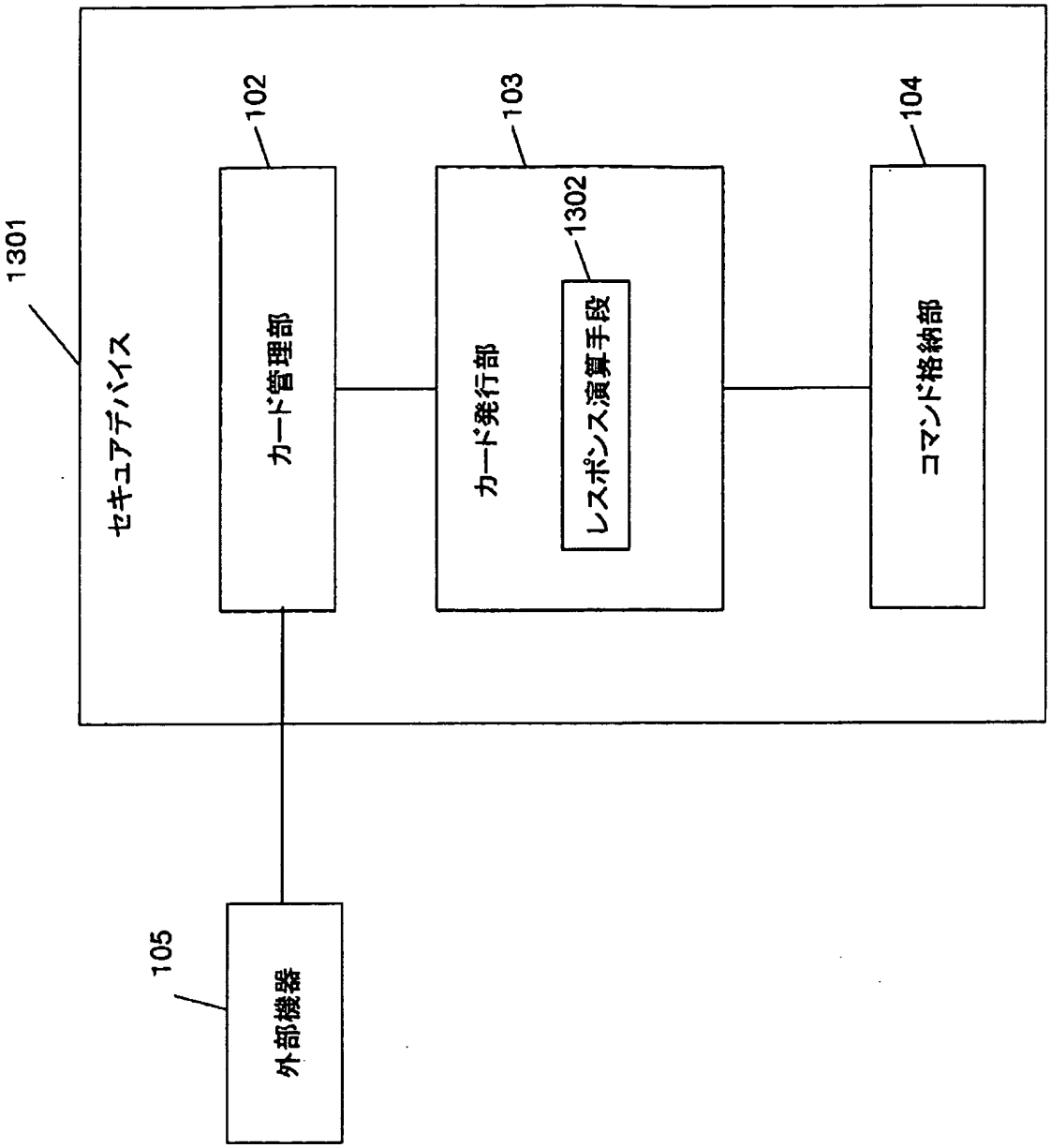

開始
レスポンス解析可能な状態
1101
レスポンス中のステータスワードが
成功を意味するかどうかを判定テーブル1201を
参照して判断する
1102
YES
レスポンスは成功
を意味するか？
NO
特権モード管理部702に特権モード解除を要求する
1103
外部機器にレスポンスを送信する
1104
終了

【図１２】

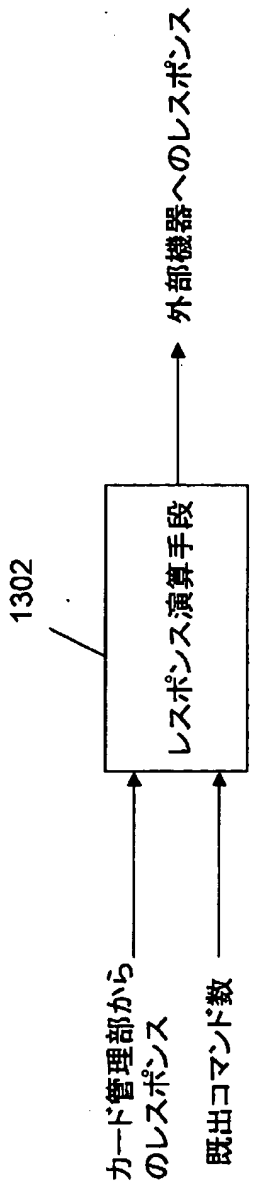
1201

ステータスワード	結果
9000h	成功
9000h以外	失敗

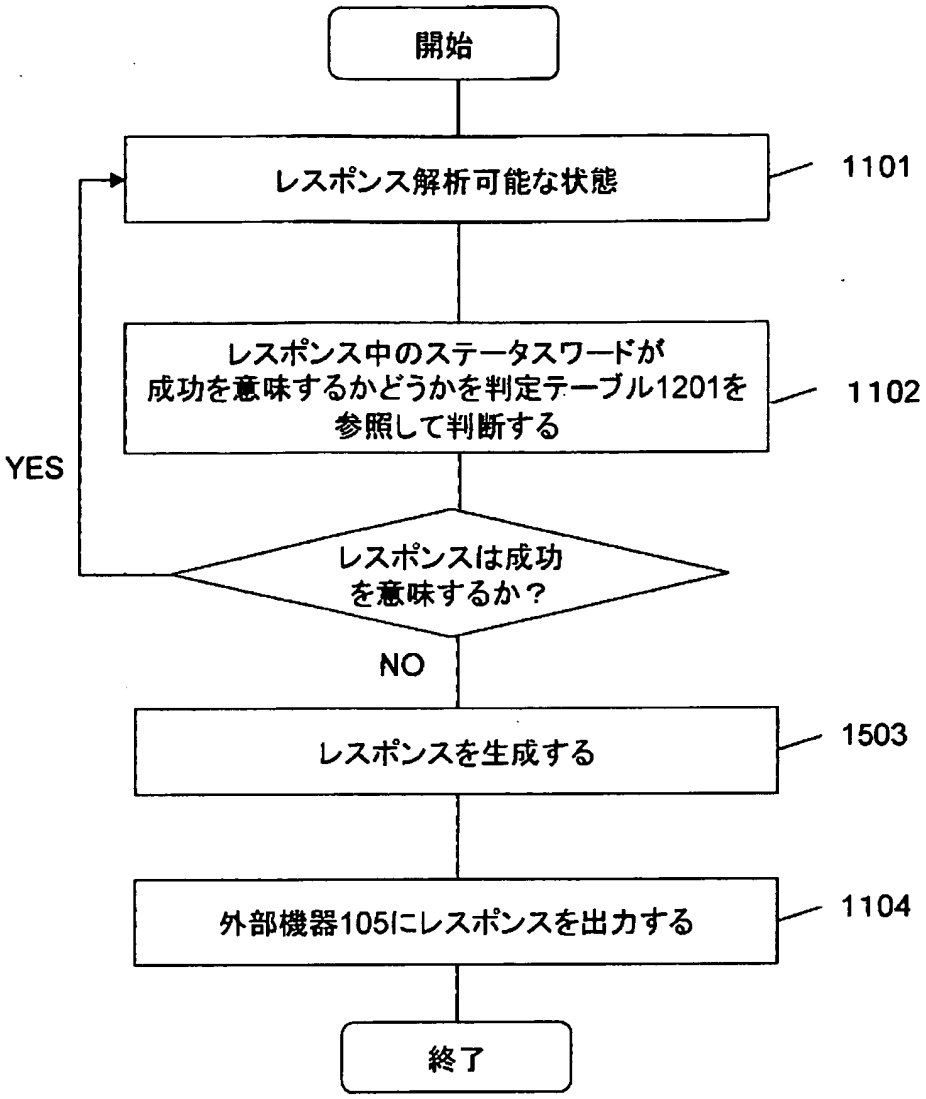
【図１３】


1301
セキュアデバイス
102
カード管理部
103
カード発行部
1302
レスポンス演算手段
104
コマンド格納部
105
外部機器

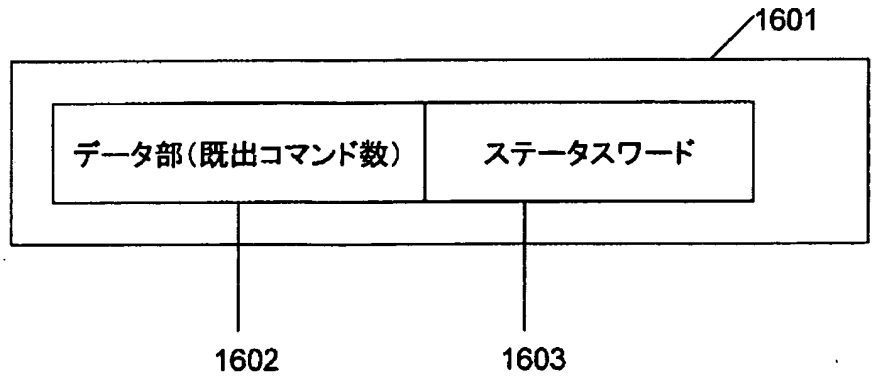
【図１４】



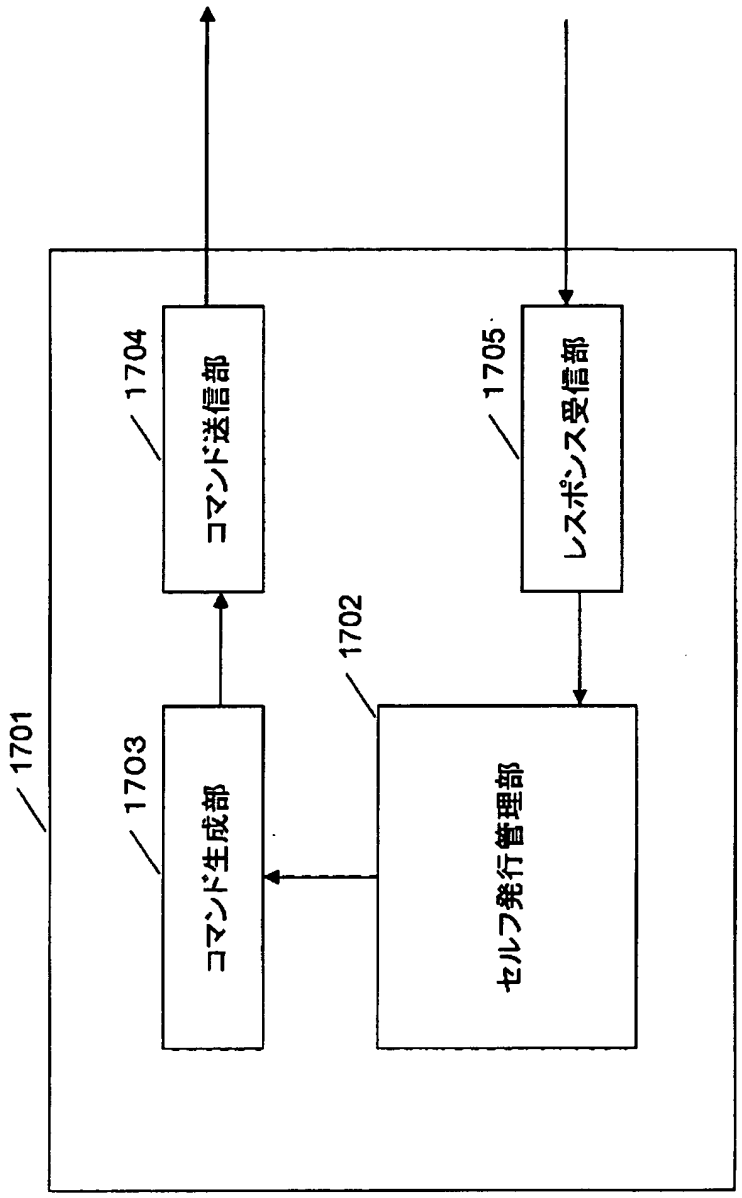
【図１５】


開始
レスポンス解析可能な状態
1101
レスポンス中のステータスワードが
成功を意味するかどうかを判定テーブル1201を
参照して判断する
1102
YES
レスポンスは成功
を意味するか？
NO
レスポンスを生成する
1503
外部機器105にレスポンスを出力する
1104
終了

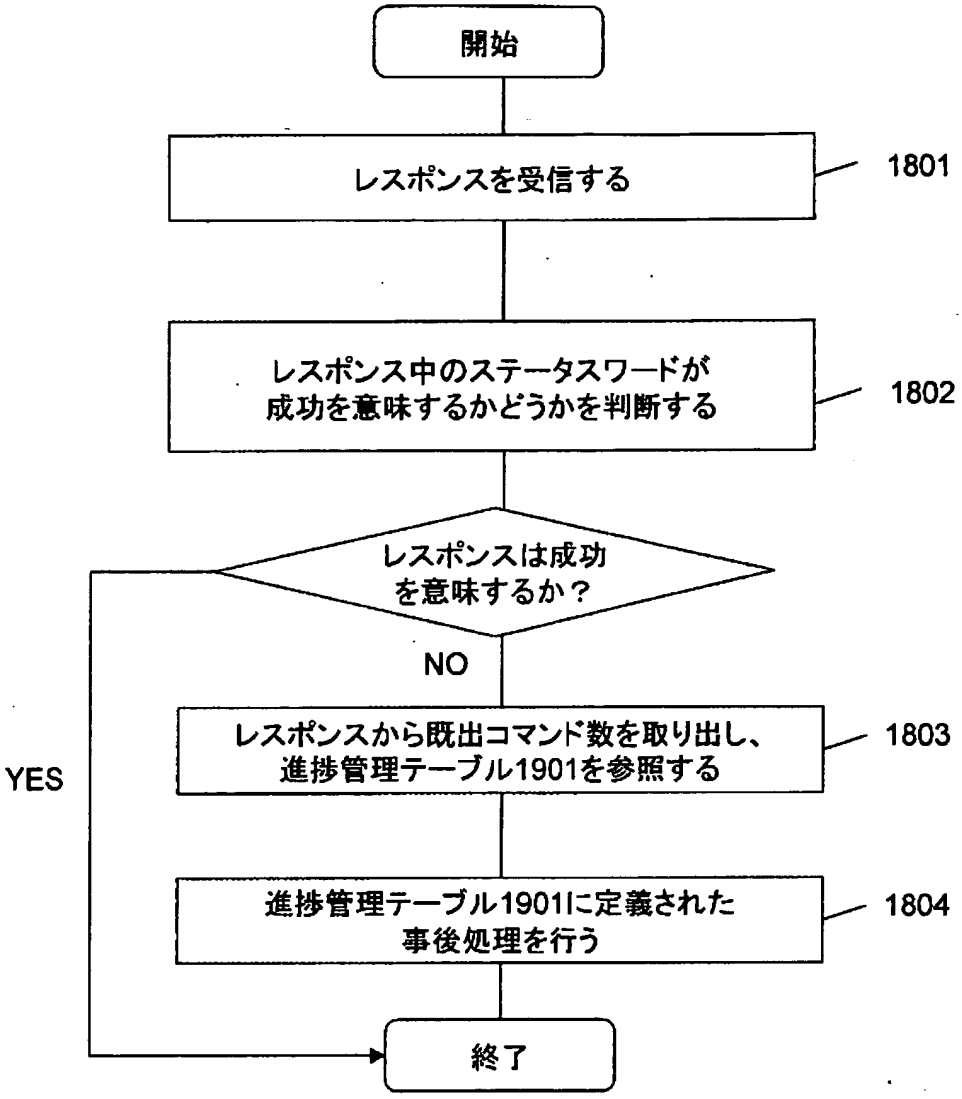
【図１６】


1601
データ部（既出コマンド数）
ステータスワード
1602
1603

【図１７】


1701
1702
1703
1704
1705
コマンド生成部
セルフ発行管理部
コマンド送信部
レスポンス受信部

【図１８】

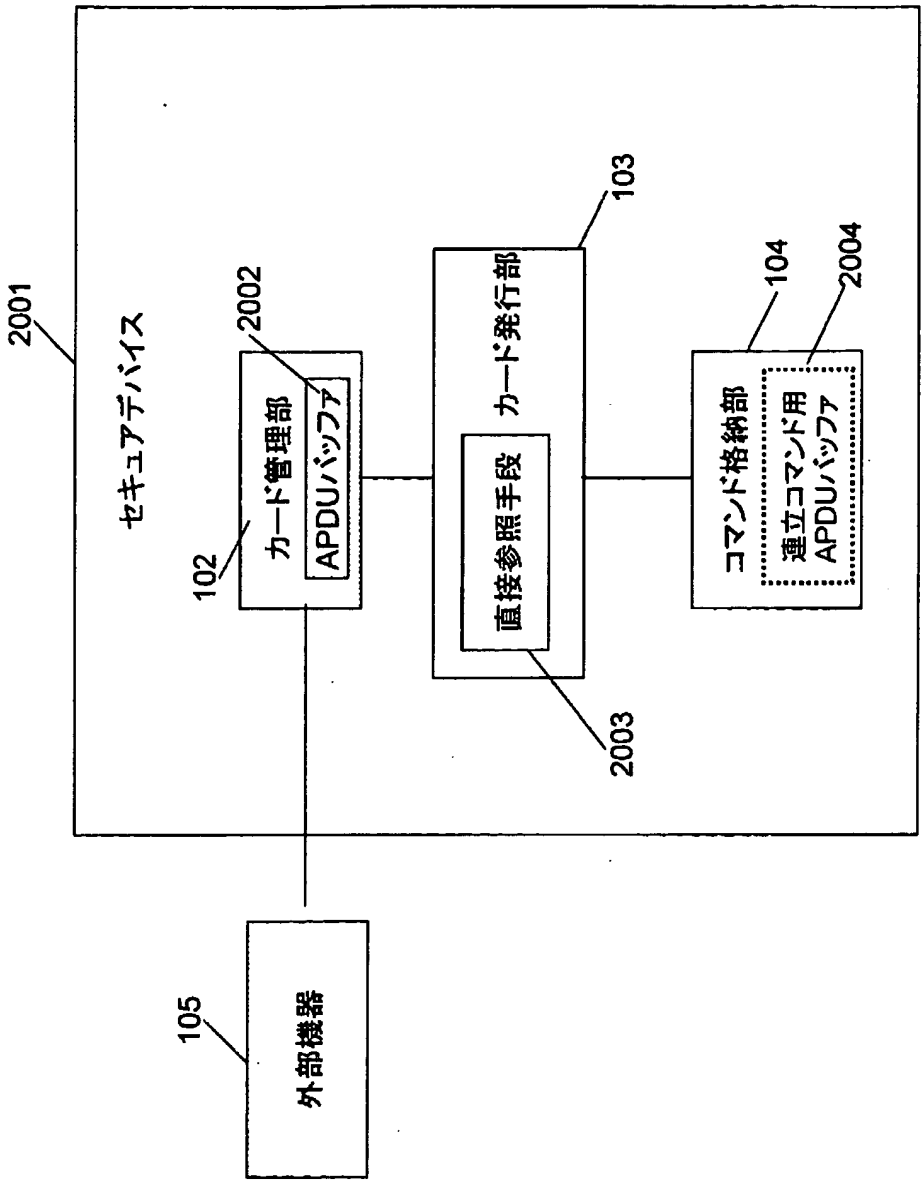

開始
レスポンスを受信する
1801
レスポンス中のステータスワードが
成功を意味するかどうかを判断する
1802
レスポンスは成功
を意味するか？
NO
YES
レスポンスから既出コマンド数を取り出し、
進捗管理テーブル1901を参照する
1803
進捗管理テーブル1901に定義された
事後処理を行う
1804
終了

【図１９】

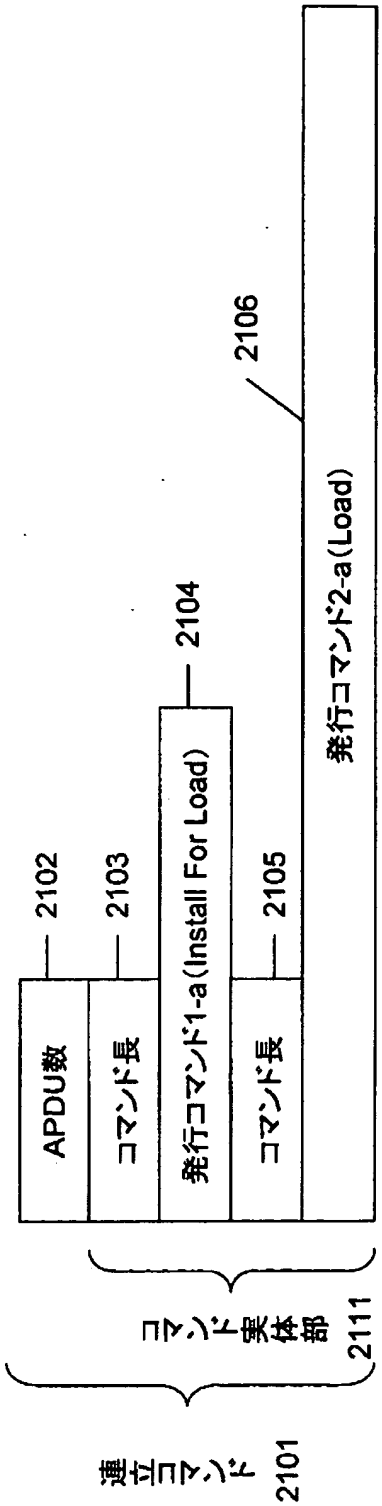
1901

既出コマンド数	エラー処理
1	×××
2	△△△
.....	....
n	カードにクリアコマンド送信

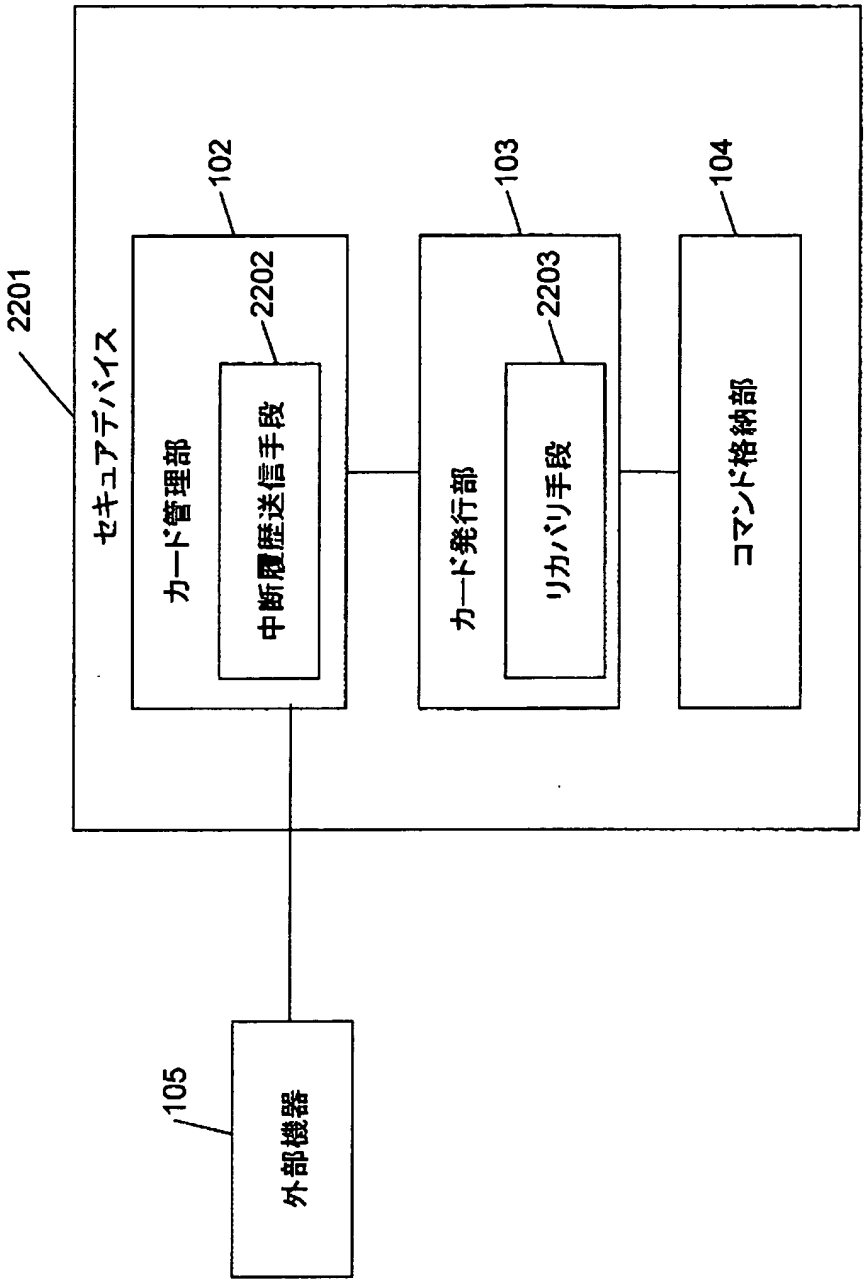
【図２０】


2001
セキュアデバイス
2002
カード管理部
APDUバッファ
102
103
カード発行部
直接参照手段
2003
104
2004
コマンド格納部
連立コマンド用
APDUバッファ
105
外部機器

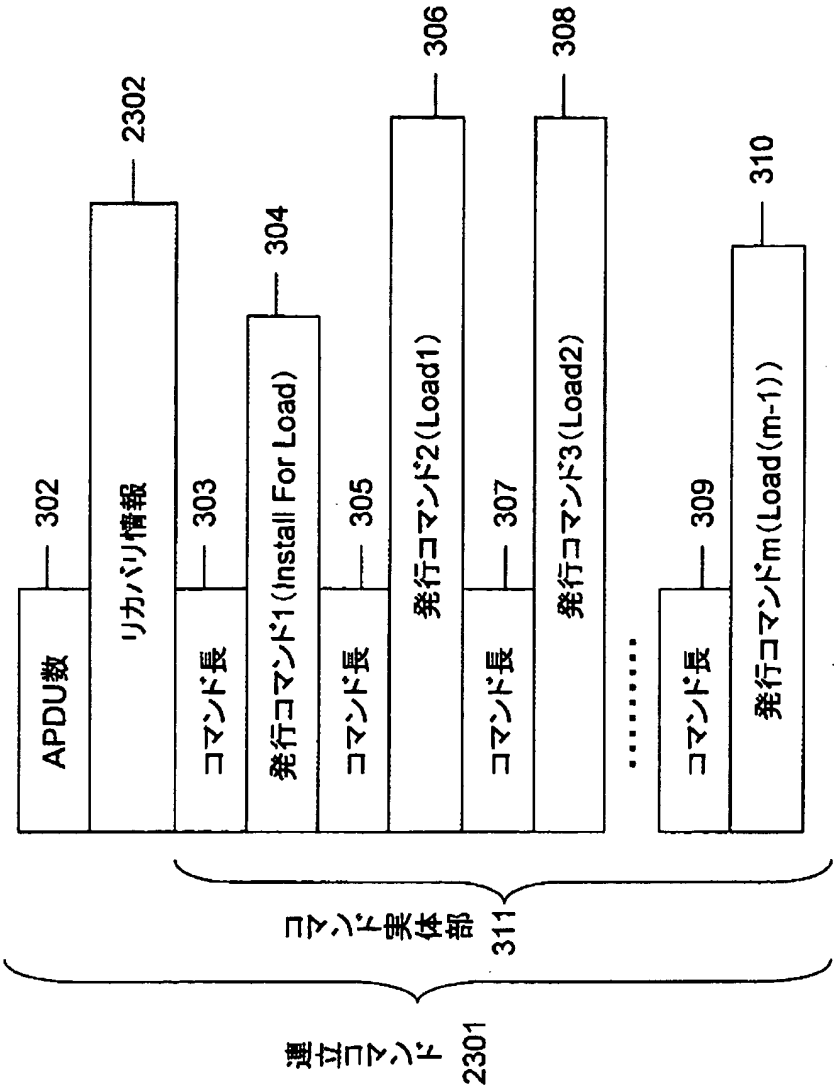
【図２１】


連立コマンド
2101
コマンド実体部
2111
APDU数
2102
コマンド長
2103
発行コマンド1-a(Install For Load)
2104
コマンド長
2105
発行コマンド2-a(Load)
2106

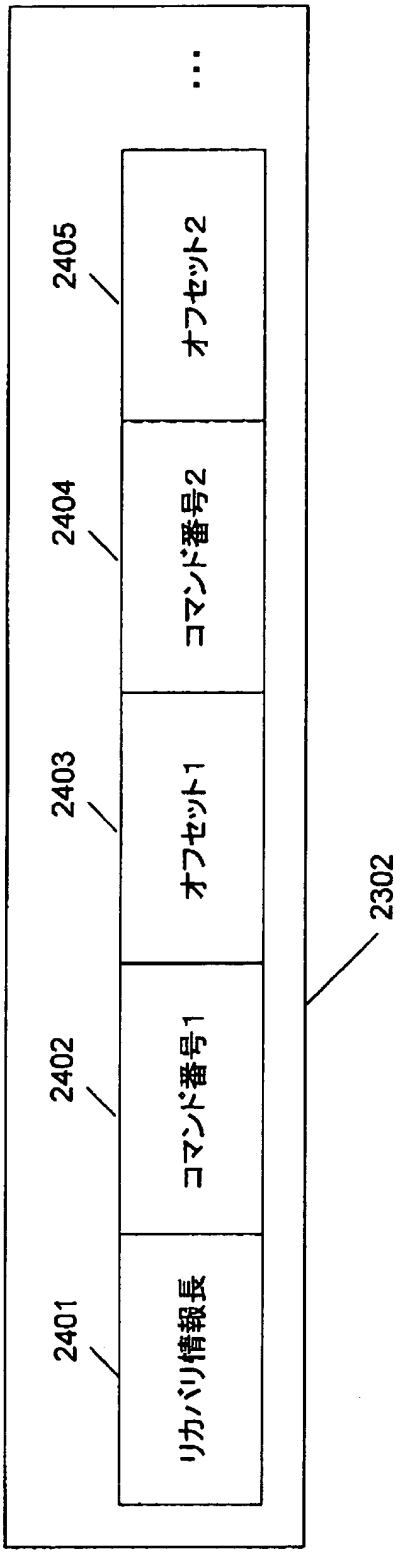
【図２２】


2201
セキュアデバイス
102
カード管理部
2202
中断履歴送信手段
103
カード発行部
2203
リカバリ手段
104
コマンド格納部
105
外部機器

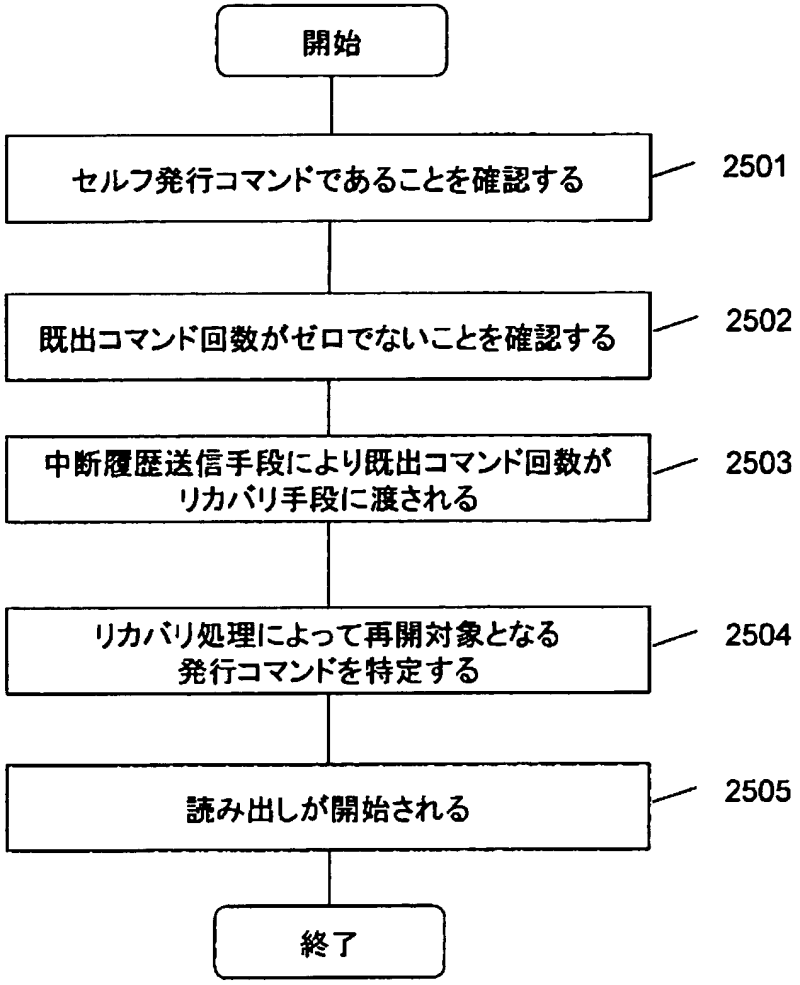
【図２３】


APDU数
302
リカバリ情報
2302
コマンド長
303
発行コマンド1(Install For Load)
304
コマンド長
305
発行コマンド2(Load1)
306
コマンド長
307
発行コマンド3(Load2)
308
.....
コマンド長
309
発行コマンドm(Load(m-1))
310
コマンド実体部
311
連立コマンド
2301

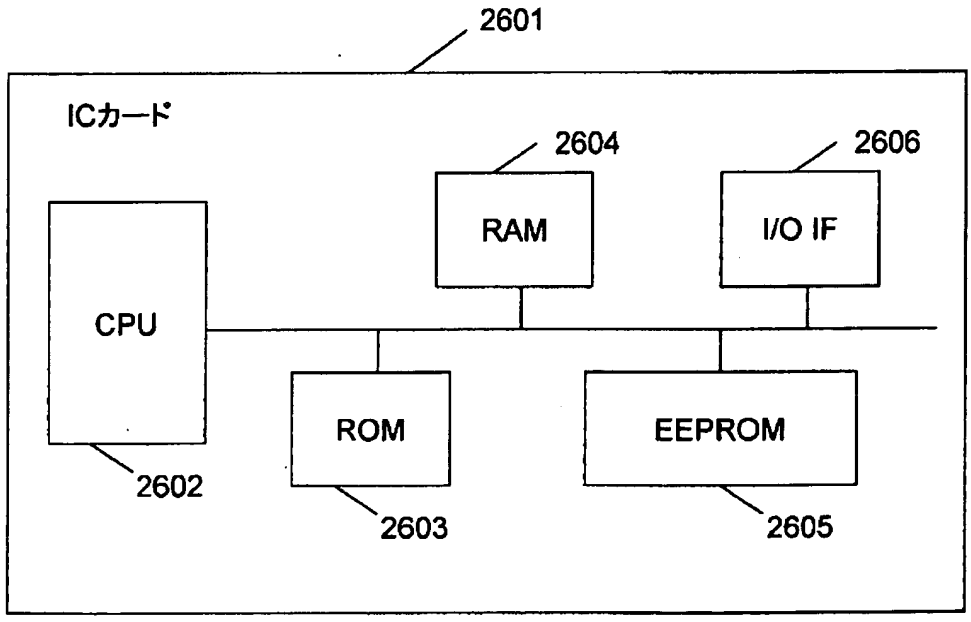
【図２４】


2401
リカバリ情報長
2402
コマンド番号1
2403
オフセット1
2404
コマンド番号2
2405
オフセット2
...
2302

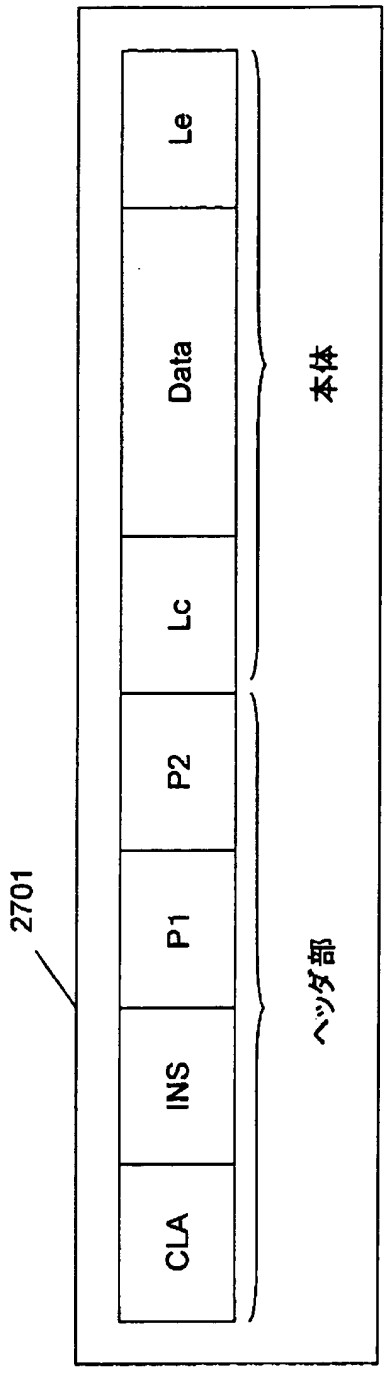
【図２５】


開始
セルフ発行コマンドであることを確認する
2501
既出コマンド回数がゼロでないことを確認する
2502
中断履歴送信手段により既出コマンド回数が
リカバリ手段に渡される
2503
リカバリ処理によって再開対象となる
発行コマンドを特定する
2504
読み出しが開始される
2505
終了

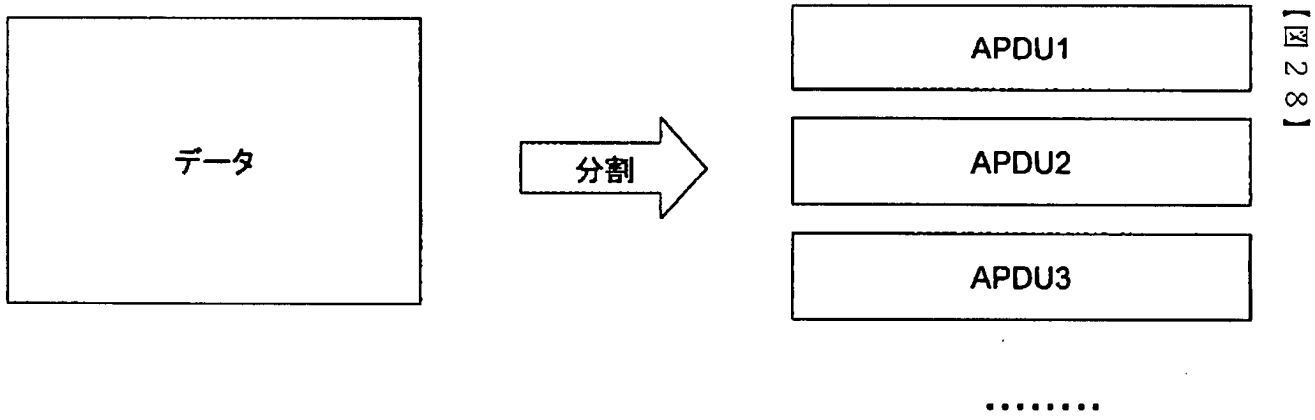
【図２６】


2601
ICカード
2604
RAM
2606
I/O IF
CPU
2602
ROM
2603
EEPROM
2605

【図２７】



【図２８】



【書類名】要約書
【要約】
【課題】セキュアデバイスへのアプリケーションダウンロードを実行する場合に通信中断による発行処理の中断を防ぐとともに、外部機器から受信したセキュリティ対策を施したデータの処理負荷を軽減させることにより、アプリケーションダウンロードの高速化を実現するための装置およびその処理方法を提供する。
【解決手段】セキュアデバイスの動作を管理するカード管理部１０２が外部機器１０５からの指示を受けた後、カード発行部１０３がコマンド格納部１０４に保持された発行用コマンド群の中から指示をみたす一連の発行コマンドを選択、構築し、カード発行部１０３とカード管理部１０２との間で通信を実行し、発行を完了する。カード管理部１０２は、発行処理結果を外部機器１０５に出力する。
【選択図】図１

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社